Universidad Nacional de La Plata

Facultad de Informática

Tesis presentada para obtener el grado de Magister en Ingeniería de Software

Mejora de Procesos como Soporte a Prácticas de Gobierno Electrónico

Tesista: *Juan Manuel Luzuriaga*

Directora: *Dra. Alejandra Cechich*

CoDirectora: *Dr. Gustavo Rossi*

Septiembre 2011

DEDICATORIA

A la sociedad argentina, y especialmente a todas aquellas personas que creen y apoyan mi trabajo profesional con la expectativa de que contribuya a una mejora para el bien común

AGRADECIMIENTOS

A Alejandra por su irrenunciable apoyo, colaboración y guía.

A mi familia por su amor y comprensión.

Al Poder Judicial de Neuquén por confiar en el Plan Estratégico Informático y darme la oportunidad de llevar adelante el programa de Gobierno Electrónico.

RESUMEN

Las expectativas que los ciudadanos, las empresas y otros grupos de interés tienen sobre el gobierno electrónico y sus aplicaciones específicas tienen un impacto en las decisiones sobre el uso de tecnologías de información y comunicación, así como en los criterios utilizados para evaluar los resultados de estas iniciativas. También las políticas existentes de e-gov revelan un entusiasmo por el potencial de las Tecnologías de la Información y las Comunicaciones (TIC) para ayudar a reformar las viejas estructuras del estado convirtiéndolas en un modelo de soporte para e-gov. Sin embargo, las relaciones y procedimientos que convierten un caso de aplicación de TICs en un ejemplo exitoso de implantación de gobierno electrónico no son muy claros.

En esta tesis, abordamos la relación entre mejora de procesos software y gobierno electrónico como una forma de establecer estructuras sólidas que produzcan servicios sustentables en bien del ciudadano. A partir de casos de estudio en el dominio de una organización judicial, establecemos recomendaciones y lecciones aprendidas junto con indicadores que constituyen un abordaje sistemático y más formal en el proceso de implantación de prácticas de gobierno electrónico. En particular, exploramos el caso de mejora de procesos relacionado a la implantación de firma y notificación electrónica.

ABSTRACT

Expectations that citizens, organizations and other actors have about e-government and its specific applications impact on the decision-making process concerning the use of Information & Communication Technology (ICT) as well as on criteria used to evaluate ICT initiatives. At the same time, e-gov policies reveal increasing enthusiasm for the potential of ICT to help restructure the State and building a basis for e-gov. However, relations and procedures that become the application of ICT into a successful e-government case are not so clear.

In this Thesis, we address the relationship between software process improvement and e-government as a way of establishing a solid foundation that might produce sustainable services for citizens. From case studies in the domain of a judicial organization, we establish recommendations and lessons learned along with some indicators, which constitute a systematic and more formal approach for implementing e-government practices. Particularly, we explore the software process improvement case as a support for e-signature and e-notification.

INDICE

1. INTRODUCCION

El uso de las TIC´s en los procesos existentes en el gobierno (administración pública), provee una oportunidad para replantearse los métodos tradicionales, procesos y salidas del sector público. En tal sentido, el esfuerzo apunta a mejorar el manejo de información, gestión del conocimiento y seguridad de la información, por nombrar algunas de las áreas involucradas en la oportunidad de mejora de procesos que podrán percibir los ciudadanos. Las aplicaciones de "Front-office", como las declaraciones de impuestos online a través del portal de la AFIP[1], de alguna manera han abierto el camino para definir una nueva interfase entre el gobierno y los ciudadanos.

En la actualidad existe un gran número de definiciones de gobierno electrónico. El espectro va desde conceptualizaciones que presentan al gobierno electrónico únicamente como la provisión de servicios públicos mediante aplicaciones en Internet hasta definiciones que caracterizan al gobierno electrónico como el uso de cualquier tecnología de información y/o comunicación (incluyendo faxes o teléfonos) en el gobierno. Este apartado presenta algunas definiciones de gobierno electrónico, siendo únicamente una pequeña muestra del gran número encontrado en la literatura reciente. En [34] se resumen las principales características encontradas en varias definiciones de gobierno electrónico[2] y se proponen algunas formas de clasificarlas:

> "*En los términos mas simples, e-gobierno es gobierno electrónico, o el uso de tecnología digital en la administración y prestación de servicios públicos, predominantemente a través de Internet*"
>
> "*Definimos e-gobierno simplemente como la prestación de servicios e información gubernamental de forma electrónica, 24 horas al día, los siete días de las semana*"

[1] http://www.afip.gov.ar/

[2] En esta tesis se referirá a e-gobierno y e-gov como términos equivalentes de gobierno electrónico.

"*E-gobierno, una palabra que se refiere al uso de Internet por el gobierno para la provisión de servicios, recolección de datos y la mejora de procesos democráticos, se ha convertido en la innovación tecnológica del momento*"

"*E-gobierno corresponde al uso de tecnología, en particular aplicaciones basadas en Internet, por dependencias gubernamentales para mejorar el acceso y la provisión de servicios públicos*"

"*Gobierno electrónico (e-gobierno) está a la vanguardia de los esfuerzos gubernamentales por proveer información y servicios a ciudadanos, empresas, empleados públicos, otras dependencias gubernamentales y organizaciones del sector terciario*"

"*El paradigma del e-gobierno enfatiza la construcción coordinada de redes, colaboración exterior y servicios al cliente*"

"*En años recientes los gobiernos han adoptado la idea de usar tecnologías de información para mejorar los servicios, una tenencia que se conoce como e-gobierno*"

"...e-gobierno, en el sentido más amplio, se refiere a una reconfiguración del sector público basada en tecnologías de información—y cómo el conocimiento, el poder y el propósito son redistribuidos a la luz de nuevas realidades tecnológicas"

"*E-gobierno se refiere a la prestación de información y servicios gubernamentales en línea a través de Internet u otros medios digitales*"

Una forma diferente de caracterizar el gobierno electrónico es listando una serie de aplicaciones, componentes o elementos que lo integran. Dentro de esta perspectiva se ha desarrollado una gran diversidad de términos en idioma inglés. Algunos ejemplos son "e-services", "e-management", "e-democracy", "e-policy", "e-transparency", "e-voting, "e-procurement", "e-rulemaking", e-commerce", "e-participation" y "e-governance". No todos estos términos tienen traducciones consensuadas al español. Esta sección resume algunas de las formas en que estudios anteriores han presentado estos elementos como constitutivos del gobierno electrónico:

- Servicios electrónicos (e-services) se refiere a la prestación de servicios públicos por medio de tecnologías de información y comunicación, especialmente Internet y otras aplicaciones de red.
- Gerencia electrónica (e-management) es el uso de tecnologías de información y comunicación para el mejoramiento de las operaciones gubernamentales, eficiencia interna y todas las labores de administración y reforma gubernamental.
- Democracia electrónica (e-democracy) se refiere al uso de tecnologías de información y comunicación para promover la participación ciudadana en sus diversas manifestaciones y sustentar las relaciones democráticas entre el gobierno, los ciudadanos y otros "stakeholders".
- Políticas públicas electrónicas (e-policy) es la creación (no necesariamente usando tecnologías de información y comunicación) de un marco legal y regulatorio que facilite iniciativas de gobierno electrónico y fomente un ambiente propicio para la sociedad de la información.

Partiendo del análisis de las definiciones y componentes encontrados en la literatura existente, en este apartado se argumenta que el fenómeno "gobierno electrónico" es multi-dimensional y por tanto es necesario conceptualizarlo como una amalgama de elementos y aplicaciones interrelacionados, los cuales no necesariamente tienen los mismos objetivos, prioridades y/o "stakeholders". Basados en la revisión y de forma similar a [33][35], se sugiere que los componentes principales de esta definición multi-dimensional deben ser: servicios electrónicos (e-services), gerencia electrónica (e-management), democracia electrónica (e-democracy), y políticas públicas electrónicas (e-policy).

Por tanto una definición de gobierno electrónico que pueda ser utilizada para entender y medir este fenómeno de forma clara y sistemática debe considerar al menos los cuatro elementos mencionados anteriormente. De forma adicional, para que una definición de gobierno electrónico sea realmente útil debe facilitar el entendimiento entre

investigadores y funcionarios públicos, es decir, debe tener bases teóricas sólidas, pero al mismo tiempo debe tener relevancia práctica.

1.1 Impacto del Gobierno Electrónico

Una forma complementaria de entender qué se puede medir y cómo se puede medir, es revisando cuáles son los impactos potenciales o beneficios que se esperan del gobierno electrónico. Resultados como mejoramiento de la calidad en la prestación de servicios públicos, eficiencia, eficacia, y transparencia, entre otros, son mencionados tanto en la literatura académica como entre funcionarios públicos de distintos niveles. Estos beneficios están en muchas ocasiones ligados a las metas y objetivos de los proyectos de gobierno electrónico y por tanto constituyen una forma de entender el impacto potencial de este tipo de iniciativas. Para su análisis, los resultados o beneficios pueden ser clasificados de distintas formas, donde una forma útil de presentar los beneficios es entendiéndolos como resultados de ciertas acciones e iniciativas de gobierno electrónico. Uno de los principales resultados potenciales del gobierno electrónico es el mejoramiento de la calidad en los servicios públicos. Esto no sólo se refiere a la conveniencia de tener acceso a información y servicios gubernamentales 24 horas del día los 7 días de la semana, sino también al mejoramiento substancial de los productos, procesos y atención a los ciudadanos.

Las labores gubernamentales son muy diversas y los recursos siempre son escasos. Una de las promesas del gobierno electrónico es elevar la productividad de las organizaciones públicas y hacer más eficiente los procesos y acciones desarrolladas por entidades gubernamentales. Para algunos estudiosos estos beneficios están ligados a transformaciones estructurales y cambios substanciales en los procesos que actualmente son utilizados. Sin embargo, algunos estudios han encontrado que la introducción de tecnologías de información tiene efectos directos en el desempeño o productividad, pero no necesariamente en las estructuras organizacionales [5][22].

En un gran número de casos, mejorar la calidad de los servicios o hacer mas eficiente las operaciones gubernamentales son sólo pasos intermedios, pues los objetivos más importantes del gobierno electrónico tienen que ver con lograr políticas públicas y programas gubernamentales más eficaces. Este beneficio es tal vez uno de los más importantes y al mismo tiempo uno de los más difíciles de medir, pues presupone la existencia de buenos indicadores de desempeño para la política o programa objetivo (Ej., salud, educación, combate a la pobreza, etc.). Estos indicadores son necesarios, pues la intención sería tener una medición base, antes de la implementación de la iniciativa del gobierno electrónico, que se pueda comparar con los resultados alcanzados con la utilización del sistema. Sin embargo, aún con estos indicadores de política pública, todavía se tiene que pensar cuidadosamente en el periodo más adecuado para realizar la medición, pues periodos muy cortos pueden no encontrar resultados debido a que el proyecto de gobierno electrónico no ha estado en funcionamiento por suficiente tiempo. De forma similar, periodos de evaluación muy largos, no permiten aislar los efectos del proyecto de gobierno electrónico, pues muchos otros factores pueden afectar los resultados de la política o programa en cuestión [37].

Un beneficio potencial, especialmente interesante para países con problemas de corrupción, es que las tecnologías de información y comunicación pueden fomentar y facilitar la transparencia de las labores gubernamentales y los procesos de rendición de cuentas [60]. El acceso y disponibilidad de información relevante sobre finanzas, recursos humanos y otros temas que hasta hace algunos años eran sólo accesibles para un selecto grupo de actores sociales, tiene el potencial de transformar radicalmente las relaciones entre el aparato administrativo del gobierno, los ciudadanos y sus representantes políticos. Sin embargo, estudios sobre votación electrónica han encontrado que las tecnologías de información pueden también tener efectos contrarios y disminuir la transparencia en procesos democráticos que solían ser realizados con poca intervención tecnológica[3].

[3] Dr. Alejandro Prince, 2005: Voto electrónico en Argentina. http://www.spkrsbr.com/biblioteca/htm/Libro_Voto_electronico_%20Prince.PDF

Para que un gobierno democrático funcione, es necesario que los ciudadanos tengan oportunidades de participar de forma real y efectiva en las decisiones públicas. Las tecnologías de información y comunicación tienen el potencial de facilitar esta participación. Algunos mecanismos específicos son foros virtuales y "chats", en donde los ciudadanos pueden expresar sus opiniones en la comodidad de sus hogares. Procesos de participación que solían ser para una minoría selecta de grupos de interés como "comentarios a regulaciones" (e-rulemaking) han comenzado a beneficiarse con opiniones de una base ciudadana más amplia. Sin embargo, las dependencias gubernamentales no siempre están preparadas para los cambios derivados de estos innovadores sistemas de participación ciudadana (Ej. el gran volumen de comentarios recibidos) y su capacidad de respuesta es limitada [23][40].

Los gobiernos no son únicamente usuarios de tecnologías de información y comunicación, sino que tienen la capacidad formal de crear normas y reglamentos que respalden y fomenten la implementación de proyectos de gobierno electrónico. Así, un beneficio adicional del gobierno electrónico es precisamente la creación de un marco regulatorio que respalde y sustente el diseño, implementación, uso y evaluación de tecnologías de información y comunicación al interior del propio gobierno y en sus relaciones con otros actores sociales. Un importante ejemplo de este tipo de regulaciones son las leyes de acceso a información gubernamental que recientemente están siendo impulsadas en un gran número de países, incluyendo a países latinoamericanos como México, Chile y Colombia [1][17][58]. Otro ejemplo son reglamentos y normas que facilitan el uso de tecnologías de información y la colaboración e intercambio de información entre diferentes dependencias gubernamentales, compañías privadas y organizaciones no gubernamentales.

De forma similar a lo descripto en el párrafo anterior, el gobierno tiene la capacidad de regular algunas de las acciones que respecto al uso de tecnologías de información y comunicación realicen otras entidades, incluyendo tanto a empresas privadas como a organizaciones no gubernamentales [28]. Por tanto un beneficio más del gobierno electrónico puede ser la promulgación de leyes (si el poder legislativo está involucrado),

reglamentos y políticas que fomenten el uso y difusión de tecnologías de información y comunicación en el marco de lo que se ha denominado la sociedad de la información. Leyes y reglamentos referentes al uso de firmas digitales y programas que impulsan la penetración de computadoras e Internet en lugares remotos o de difícil acceso constituyen ejemplos de este tipo de beneficios. Otros ejemplos de este tipo de políticas de gobierno pueden encontrarse de forma abundante en el programa e-México[4], que incluye políticas para incrementar la cobertura de Internet en el país, políticas para fomentar el desarrollo de la industria de Tecnologías de Información, etc.

A diferencia de organizaciones privadas, el gobierno es creado y opera bajo un marco legal que promueve ciertas acciones y prohíbe otras. El marco legal no solo promueve directrices, sino que determina y enmarca totalmente lo que hace el gobierno, siendo obligatorio. Las iniciativas de gobierno electrónico no están exentas de este tipo de influencias y las leyes y reglamentos se pueden convertir en grandes incentivos y catalizadores, pero también, en circunstancias menos afortunadas, en poderosas barreras y retos muy difíciles de ser superados [7][13][20][30][38][48]. Algunos ejemplos de este tipo de determinantes son: los ciclos anuales de presupuestación; las relaciones intergubernamentales entre los poderes ejecutivo, legislativo y judicial; y la relativa autonomía con la que operan las dependencias, derivada de la escasez de incentivos para la colaboración inter-organizacional [10][14][21][38]. Las iniciativas de gobierno electrónico se deben evaluar teniendo en consideración esta y otras diferencias con respecto al sector privado.

Los gobiernos y las iniciativas de gobierno electrónico no se encuentran en el vacío, sino que operan en contextos sociales, económicos y políticos concretos [21][30][46]. Estas condiciones contextuales también afectan las iniciativas de gobierno electrónico, si bien los impactos no son necesariamente directos [32]. Hay dos importantes ejemplos de determinantes contextuales del gobierno electrónico. El primero lo constituyen las presiones políticas y de agenda gubernamental, que tienen un impacto tanto en la selección como en la implementación y evaluación de iniciativas de gobierno

[4] www.e-mexico.gob.mx/

electrónico [10][30][56]. El segundo determinante son las expectativas ciudadanas por servicios de gobierno electrónico [32][49][61][62][63]. Las expectativas que los ciudadanos, las empresas y otros grupos de interés tienen sobre el gobierno electrónico y sus aplicaciones específicas tienen un impacto en las decisiones sobre el uso de tecnologías de información y comunicación, así como en los criterios utilizados para evaluar los resultados de estas iniciativas. En la mayoría de los casos, los autores han usado análisis estadístico para dar sustento a sus conclusiones. Por ejemplo, en el caso de las expectativas ciudadanas o demanda del gobierno electrónico, la mayoría de los autores han usado información disponible de encuestas realizadas por ellos mismos o por alguna organización. La demanda ha sido operacionalizada usando indicadores como ingreso, educación, acceso a computadoras y acceso a Internet, entre otras.

Si observamos a lo largo del mundo las aplicaciones de e-gov, podremos apreciar cómo los gobiernos proveen servicios hacia sus ciudadanos, de una manera más eficiente y efectiva. Esta realidad ha hecho que en los países desarrollados y en vías de desarrollo los proyectos de e-gov estén presentes en la agenda de los gobernantes. La Comisión Europea tradicionalmente ha incluido en la agenda de e-gov los conceptos de eficiencia y efectividad: "e-gov es el uso de las tecnologías de información y las comunicaciones en la administración pública combinadas con el cambio organizacional y adquisición de nuevas habilidades para mejorar el servicio público y el proceso democrático, fortaleciendo el soporte a las políticas públicas"[5], esta agenda incita al desarrollo de los servicios existentes hacia la audiencia disponible en internet [15]. El Banco Mundial tiene una definición "instrumental" similar para e-gov: "e-gov se refiere al uso de las agencias gubernamentales de las tecnologías de información que tienen la habilidad para transformar la relación con los ciudadanos, negocios y otros brazos de gobierno, dichas tecnologías pueden servir con diferentes fines: mejorar el servicio del gobierno hacia sus ciudadanos, mejorar la interacción en los negocios y la industria, aumentar los recursos del ciudadano en cuanto al acceso a la información, o una administración gubernamental más eficiente. El beneficio resultante debe ser menor corrupción, mayor

[5] http://ec.europa.eu/information_society/tl/soccul/egov/index_en.htm

transparencia, mayor comodidad, crecimiento de los ingresos, y/o reducción de costos"[53].

Estos extractos de informes sobre políticas existentes de e-gov revelan un entusiasmo por el potencial de las TIC´s para ayudar a reformar las viejas estructuras del estado convirtiéndolas en un modelo de e-gov [12][47]. Rossel y Finger [57] plantearon el desafío de ubicar al Estado como un proveedor de servicios, pero la cuestión aquí es el amplio rol del sector público para proveer un espacio para los ciudadanos y otros miembros de la comunidad para interactuar con los servidores públicos (y sus instituciones).

1.2 Objetivos

En el contexto descripto en la sección anterior y desde el dominio de las TIC, el objetivo de este trabajo es *desarrollar guías y experiencias para la aplicación de mejora de procesos en ámbitos gubernamentales que sirvan de soporte a la inclusión de prácticas de gobierno electrónico.*

Objetivos específicos:

a. Proponer guías de para la aplicación de mejora de procesos en el marco de organizaciones gubernamentales

b. Establecer relaciones entre las guías para la aplicación de mejora de procesos y la inclusión de prácticas de gobierno electrónico – en particular firma electrónica.

c. Validar la propuesta en caso de estudios reales analizando lecciones aprendidas.

1.3 Metodología

En esta tesis se han combinado técnicas que provienen de la mejora de procesos software y de prácticas para gobierno electrónico. Se ha trabajado bajo el paradigma de investigación-acción (I-A) que ha obtenido una amplia aceptación y aplicación en la investigación en ingeniería del software en los últimos años. Este método presenta como principales características: orientación a la acción y al cambio, focalización en un problema, un modelo de proceso "orgánico" que engloba etapas sistemáticas y algunas veces iterativas, y la colaboración entre los participantes. De las diferentes variantes de la I-A, aplicaremos la denominada "participativa". Este método permite generar un beneficio al "cliente" de la investigación y, al mismo tiempo, generar "conocimiento de investigación" relevante. Por tanto, Investigación-Acción es una forma de investigar de carácter colaborativo que busca unir teoría y práctica entre investigadores y profesionales mediante un proceso de naturaleza cíclica.

También en el marco de esta tesis se ha realizado el diseño e implementación de un caso de estudio para comprobar la aplicabilidad de nuestra propuesta. Los casos de estudio se utilizan para monitorizar proyectos, actividades o asignaciones. En este tipo de estrategia, los datos se recogen para un propósito específico. Un caso de estudio está orientado normalmente a analizar un determinado atributo o establecer relaciones entre diferentes atributos.

1.4 Contexto

Esta tesis se desarrolló en el contexto de tres proyectos de investigación:

- Proyecto UNCo (Universidad Nacional del Comahue) 04/E059. Título del proyecto: "Mejora del Proceso de Desarrollo de Software Basado en Componentes". Dirigido por la Dra. Alejandra Cechich, en el período 01-01-2005 al 31-12-2007.

- Proyecto UNCo (Universidad Nacional del Comahue) 04/E072. Título del proyecto: "Identificación, Evaluación y Uso de Composiciones Software". Dirigido por la Dra. Alejandra Cechich, en el período 01-01-2008 al 31-12-2012.
- Proyecto CompetiSoft – Mejora de procesos para fomentar la competitividad de la pequeña y mediana industria del software en Iberoamérica. Proyecto CyTED 3789. http://alarcos.inf-cr.uclm.es/Competisoft/index.aspx (2005-2008).

1.5 Estructura de la Tesis

En el capítulo 2 se presentan las nociones básicas del problema de estudio, como fundamentos para el desarrollo de esta tesis. Se presentan particularidades de la mejora de procesos y del gobierno electrónico, estableciendo relaciones e interacciones entre ellos.

En el capítulo 3 se describe la propuesta de mejora para gobierno en el caso de estudio a partir del cual se elaboran guías y lecciones aprendidas.

En el capítulo 4 se realiza la aplicación de prácticas de gobierno electrónico – en particular firma y notificación electrónica – a partir de la base de soporte generada mediante la mejora de procesos.

Finalmente, en el capítulo 5 se presentan conclusiones, las principales contribuciones de la tesis y los trabajos futuros.

2 MEJORA DE PROCESOS COMO SOPORTE AL GOBIERNO ELECTRÓNICO: FUNDAMENTOS DE LA TESIS

Los retos que afrontan las organizaciones productoras de software en la actualidad las obligan a ser más competitivas y a plantearse los nuevos mercados que supone la oportunidad que da la globalización de nuestra economía. Para ello, muchas veces deben adecuar su forma de trabajar para ser capaces de afrontar los nuevos desafíos. Una vez tomada la decisión, la implementación de un Sistema de Calidad permite mejorar los procesos internos y minimizar el riesgo de no cumplir con las expectativas de los Clientes y del mercado respecto al producto o servicio que la organización ofrece. Las organizaciones gubernamentales no escapan a este paradigma de mejora, dado que a través del gobierno electrónico, como veremos mas adelante, se busca ampliar y mejorar la capacidad de servicios al ciudadano.

Cada organización posee procesos operativos que son esenciales para el desarrollo de sus actividades. El crecimiento de la organización depende de su capacidad de descubrir fortalezas, debilidades y oportunidades de mejora en su actividad. El enmarcar dicha actividad en un Modelo de Calidad sienta las bases para su futuro crecimiento sustentable. A través de la formalización de sus procesos se logra conocer lo que se hace, y luego de la medición del proceso, conocer cómo se hace, en pos de mejorar respecto al pasado conocido.

La Calidad es muchas veces identificada como algo superior, excelente, libre de deficiencias, capaz de cubrir las necesidades y expectativas de los Clientes. Esta idea del significado de Calidad es muchas veces intimidante para una organización pequeña sin acceso a consultoría sobre el tema. Algunas definiciones de calidad son:

- Definición de la norma ISO 9000 [52] “La Calidad es el grado en el que un conjunto de características inherentes cumple con los requisitos”.

- Real Academia de la Lengua Española[6]: "Propiedad o conjunto de propiedades inherentes a una cosa que permiten apreciarla como igual, mejor o peor que las restantes de su especie".
- Walter A. Shewhart [59]: "La calidad es el resultado de la interacción de dos dimensiones, la dimensión subjetiva (lo que el cliente quiere) y la dimensión objetiva (lo que se ofrece)".

De las definiciones anteriores podemos inferir que la Calidad no es la búsqueda de la excelencia absoluta, sino lograr el grado de excelencia óptimo de un producto, proceso o servicio para que cumpla su cometido de manera eficiente.

2.1 La Calidad en el Proceso de Desarrollo de Software

En relación al Proceso de Desarrollo de Software, la calidad es un parámetro, que junto a los parámetros tiempo, alcance y costo definen el resultado de un producto, y a su vez, del proceso que lo crea. En relación a estos cuatro parámetros antes mencionados podemos decir que:

- El tiempo se refiere a la cantidad disponible para completar un proyecto.
- El costo se refiere al monto presupuestado para el proyecto.
- El alcance se refiere a lo que se debe hacer para producir el resultado final del proyecto
- La calidad, tomando la definición de Walter A. Shewhart [59], es la medida de satisfacción del Cliente (dimensión subjetiva), en relación a la conjunción del proceso de construcción utilizado y los parámetros tiempo, costo y alcance (dimensión objetiva).

[6] www.rae.es/

Estos cuatro parámetros son frecuentemente competidores entre sí. Incrementar el alcance típicamente aumenta el tiempo y el costo; una restricción fuerte de tiempo puede significar un incremento en costos y una reducción en los alcances; y un presupuesto limitado puede traducirse en un incremento en tiempo y una reducción de los alcances. Entre estas competencias entre parámetros, la calidad es inversamente proporcional a los otros tres, tanto en dimensión subjetiva (satisfacción del cliente) como en dimensión objetiva (costo, tiempo y alcance).

Entonces, la correcta medida o justa relación entre los cuatro parámetros que suscriben la creación de un producto se encuentra dada por el proceso que gestiona su creación.

Para la industria de software existen numerosos modelos de mejora de calidad de proceso aplicables, cuyos resultados [6][16][45][51][64] son variados. Todos los estudios concuerdan en los beneficios y las dificultades de implantar las mejores prácticas propuestas por los modelos, debido a factores endógenos y exógenos que afectan a las organizaciones, entre los cuales se cuentan: tamaño de la organización, sus objetivos a mediano y largo plazo y el proceso de desarrollo aplicado actualmente. Por otro lado, la implantación de los modelos comerciales disponibles en una organización exige estructuras de personal capaces de soportar la diversidad de tareas, además de un conjunto de competencias por recurso altamente exigentes. En el caso de la Pequeña y Mediana Industria (PyME), la elección e implantación de un Proceso de Mejora exige una fuerte inversión en costo, tiempo y recursos, además de una visión a largo plazo.

Los Modelos de Mejora de Calidad de Proceso como CMMI[7], los estándares como la familia ISO[8] y el modelo CompetiSoft[9] fueron creados con el fin de lograr éxitos repetibles y prácticas avaladas por el resto de la organización. Entre éstos, CompetiSoft se destaca por haber sido concebido para organizaciones pequeñas dedicadas al desarrollo de software.

[7] www.sei.cmu.edu/cmmi/

[8] www.iso.org/

[9] alarcos.inf-cr.uclm.es/Competisoft/

Toda organización dedicada a la manufactura de productos posee un conjunto de actividades probadas que satisfacen en mayor o mayor medida su necesidad de respuesta a los requerimientos de sus clientes. La ejecución y dependencia de dichas actividades conforma el proceso de construcción que la organización practica. Este proceso genera en los trabajadores un marco laboral conocido y difundido, y en general es la base de la subsistencia de la organización.

En la industria del desarrollo de software, la innovación y el desafío son elementos presentes en cada proyecto. La fuerza laboral de una organización de este tipo se caracteriza por manejar con soltura las tecnologías de la información y comunicación, poseer suficientes destrezas en el uso y generación de información, ser proactiva en el aprendizaje, y por último pero no menos importante, estar interesada en la calidad mas que la cantidad, contribuyendo a la mejora y la innovación. Por lo expuesto anteriormente, la adopción de un proceso de mejora es un paso lógico para el crecimiento de la organización y sus integrantes.

A su vez, la calidad de los productos y servicios ofrecidos en la actualidad se encuentra estrechamente relacionada al proceso del cual forman parte. El florecimiento de la mano de obra especializada (o trabajadores del conocimiento) trae aparejada una diversidad de buenas prácticas y métodos que en determinados entornos fueron o son efectivos, pero que raras veces se encuentran documentados y catalogados según su efectividad.

La decisión sobre la adopción de un modelo de mejora en una PyME es desafiante. Por un lado, los modelos disponibles son numerosos. Si bien difieren respecto a la metodología a aplicar, todos buscan mejorar la capacidad de gestión de una organización a través de la formalización de procesos. En contraste, la mayoría de los modelos comerciales carecen de explicaciones claras sobre los cambios a realizar en una organización para lograr el cometido. La consultoría para la aplicación de modelos de mejora es costosa, y las estructuras necesarias en la organización son grandes y muy difíciles de mantener debido a la complejidad de los modelos. La mayoría fueron creados para organizaciones de gran escala, con estructuras organizacionales que abarcan todas las disciplinas necesarias para el desarrollo de las actividades propuestas.

El propósito de la adopción de un modelo de mejora es caracterizar la práctica actual, identificando debilidades y fortalezas, y la habilidad del proceso para controlar o evitar las causas de baja calidad, desviaciones en coste o planificación. La adopción de una iniciativa de mejora en el proceso de software asiste a las organizaciones en lograr una visión compartida de su actividad, enmarcando la misma en un estándar conocido y avalado. Con ello, las organizaciones persiguen:

- Frecuentar éxitos obtenidos de prácticas repetibles.
- Reducir los riesgos asociados a su actividad.
- Mejorar los canales de comunicación de los integrantes del Equipo de Desarrollo, logrando el entendimiento sobre los objetivos a alcanzar en cada etapa o hito del proyecto.

2.2 Modelos de Mejora de Procesos

2.2.1 El Modelo Capability Maturity Model Integration (CMMI)

El modelo CMMI (Modelo de Madurez de Capacidad Integrado) [45] fue creado por la Universidad Carnegie Mellon de Pittsburgh como método para evaluar el nivel de madurez del proceso de desarrollo del software de una organización u organismo. El proceso se evalúa mediante un cuestionario y las respuestas sirven para determinar una magnitud denominada "Nivel de Madurez del Proceso".

En principio fue creado para evaluar y mejorar la capacidad de los contratistas de software del Departamento de Defensa de los Estados Unidos. Con el tiempo el modelo CMMI se convirtió en un alto estándar de Ingeniería de Software en el mundo para todo tipo de compañías. Se encuentra fundamentado en prácticas reales de las compañías mas avanzadas, y refleja las mejores prácticas en procesos de desarrollo de software.

El Modelo CMMI se compone de 316 prácticas claves agrupadas en 18 áreas y distribuidas en una jerarquía de cinco niveles, a través de los cuales una organización progresivamente alcanza mayor calidad, productividad y menores costos en el

desarrollo de software. Los niveles progresan desde el 1, que representa el estado elemental, hasta el nivel 5, que representa el estado de optimización continua.

Como muestra la Figura 1 los cinco niveles de madurez del proceso son:

1. *Inicial*: la organización no dispone de procesos y controles definidos. Se trabaja con procedimientos que no están normalizados, es decir, procedimientos tanto del propio desarrollo de software como de su planificación y control, que no están establecidos explícitamente antes de su uso. Por otro lado las técnicas y/o herramientas que se emplean para el desarrollo del software carecen de una integración entre las mismas y únicamente son empleadas en algunas fases del ciclo de vida del software. La característica de las organizaciones que se encuentran en este nivel es la carencia de un control efectivo de la Gestión de Proyectos de Software. Puede suceder que la organización disponga de procedimientos y técnicas formales de gestión del proceso de desarrollo establecido y de herramientas, pero éstas no son utilizadas de manera estándar en todos los proyectos.
2. *Repetible*: la organización posee métodos estandarizados, logrando de esta forma procesos repetibles. Las organizaciones que se encuentran en este nivel son las que disponen de un control básico de la Gestión de Proyectos, Gestión de Calidad y Gestión de la Configuración. El mayor problema en este tipo de organizaciones sucede al introducir algún cambio o nueva tecnología en el desarrollo de un producto o servicio, por el alto grado de riesgo al fracaso.
3. *Definido*: la organización monitoriza y mejora sus procesos. Las organizaciones que se encuentran en este nivel se caracterizan por disponer de un grupo de individuos dedicados a la Gestión de Procesos, cuyo objetivo es el de mejorar el proceso de software, además de una metodología de desarrollo de software que describe las actividades técnicas y de gestión requeridas para la adecuada ejecución del proceso.
4. *Gestionado*: la organización posee controles avanzados, métricas y posee mecanismos de retroalimentación sobre la aplicación del proceso. Las

organizaciones que han alcanzado este nivel disponen de un control de los costes y calidad de las principales etapas del proceso. Es prerrequisito que exista una metodología de desarrollo software para realizar una medición efectiva.

5. *Optimizado*: la organización emplea métricas con propósitos de optimización. En este nivel, las organizaciones se encuentran en un proceso de mejora continua. Se usan todos los procesos y técnicas modernas, lo mismo que administración cuantitativa. Las organizaciones se enfocan en la mejora a través de técnicas y procesos de prevención de defectos, cambios en tecnología y cambios en procesos.

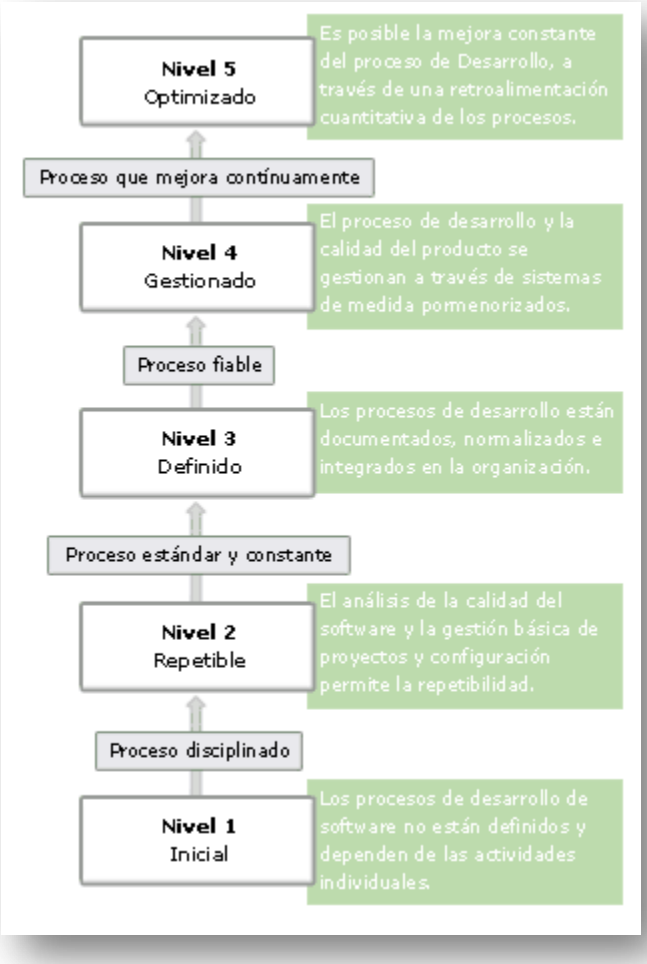


Figura 1. Esquema del Modelo CMMI

Con la excepción del nivel 1, cada nivel de madurez se descompone en varias Áreas de Procesos Claves (KPA). Cada área se organiza en cinco secciones llamadas Características Comunes (CF). Las CF especifican las Prácticas Claves (KP) que, cuando se encaminan colectivamente, cumplen los objetivos del área del proceso clave.

Cada Área de Proceso Clave identifica un conjunto de actividades claves relacionadas que, cuando se hacen en forma conjunta, alcanzan los objetivos considerados importantes para mantener la capacidad del proceso. El adjetivo "claves" implica que hay áreas del proceso que no lo son para alcanzar un nivel de madurez.

Todos los objetivos de una KPA deben alcanzarse para que la organización satisfaga esa KPA. Los objetivos resumen las KP de las KPA y pueden usarse para determinar si una organización o proyecto ha implementado efectivamente el Área de Proceso Clave. Los objetivos de las KP representan el ámbito, límites e intención de cada KPA.

Las prácticas específicas a ser ejecutadas en cada KPA evolucionarán a medida que la organización alcance mayores niveles en el Proceso de Madurez. Las Características Comunes (CF) son atributos que indican si la implementación e institucionalización de una KPA es efectiva, repetible y duradera. Las cinco CF son:

1. Acuerdo para hacer: describe las acciones que la organización debe realizar para asegurar que el proceso sea establecido y que perdure (políticas organizacionales, avales de la alta dirección, etc.).
2. Posibilidad de hacer: describe las precondiciones que deben existir en el proyecto u organización para implementar el proceso de software de manera competente (entrenamientos, recursos, etc.).
3. Actividades realizadas: describe los roles y procedimientos necesarios para implementar una KPA. Involucra establecer planes, hacer el trabajo, controlarlo y tomar acciones correctivas de ser necesario.
4. Medición y análisis: describe la necesidad de medir el proceso y analizar las medidas.

5. Verificar la implementación: describe los pasos para asegurar que las actividades se realizan de acuerdo al proceso establecido. Involucra revisiones y auditorías para asegurar la gestión y la calidad del software.

Tabla 1. Áreas de Proceso Clave del Modelo CMMI por Categoría.

N. de madurez de la organiz.	Centrado en	Areas de Proceso	Categoría
5. Optimizado	Mejora continua del proceso	-Análisis y resolución de causas de desviaciones. -Innovación y despliegue a toda la organización	Soporte G. Proceso
4. Gestionado cuantitativamente	Control cuantitativo del proceso	-Gestión cuantitativa de los proyectos. -Entendimiento cuantitativo del rendimiento de los procesos de la organización.	G. Proyecto G. Proceso
3. Definido	Proceso caracterizado por la organización y proactivo	-Desarrollo de los requisitos -Soluciones técnicas -Integración de productos -Verificación -Validación -Enfoque de procesos en organización -Definición de procesos en organización. -Entrenamiento y formación -Gestión integrada de proyectos -Gestión del riesgo -Análisis y resolución de las decisiones -Entorno organizativo para la integración -Equipo para desarrollo integrado	Ingeniería Ingeniería Ingeniería Ingeniería Ingeniería G. Proceso G. Proceso G. Proceso G. Proyecto G. Proyecto Soporte Soporte G. Proyecto
2. Gestionado	Gestión básica del proyecto	-Gestión de requisitos -Planificación de proyectos -Monitorización y control de proyectos -Gestión de acuerdos con proveedores. -Medición y análisis -Aseguramiento de la calidad del producto y del proceso -Gestión de la configuración	Ingeniería G. Proyecto G. Proyecto G. Proyecto Soporte Soporte Soporte
1. Inicial	Proc. impredecible, control reactivo		

Las Prácticas Claves (KP) describen la infraestructura y las actividades que más contribuyen a la institucionalización e implementación efectiva de una KPA. Cada KP consiste de una única sentencia, generalmente seguida de una descripción más detallada

(sub-práctica), que incluye ejemplos y elaboración. Esas KP establecen las políticas fundamentales, los procedimientos y las actividades para la KPA.

La Tabla 1 muestra las KP por Nivel de Madurez del Proceso y las categoría a la que se encuentra dirigida dicha KP.

Puntos fuertes y débiles del Modelo CMMI

Sin lugar a duda la difusión y utilización el Modelo CMMI ha sido de mucha utilidad a la Industria del Software. Éste sentó una sólida base en lo referente a metodología de trabajo, aún sin la consultoría necesaria para su aplicación en las organizaciones.

Entre sus fortalezas podríamos destacar [25][59]:

- Inclusión de las prácticas de institucionalización, que permiten asegurar que los procesos asociados con cada área de proceso sean efectivos, repetibles y duraderos.
- Guía paso a paso para la mejora, a través de niveles de madurez y capacidad (frente a ISO).
- Transición del aprendizaje individual al aprendizaje de la organización por mejora continua, lecciones aprendidas y uso de bibliotecas y bases de datos de proyectos mejorados.

En [42] podemos ver influencias positivas de CMMI en el proceso de mejora, como qué prácticas genéricas y áreas de proceso de ingeniería aportan un camino de mejora de la capacidad de cada área de proceso en la representación continua, respuesta rápida y guiada a nuevas demandas de las necesidades del negocio, o la inicial priorización de los esfuerzos, o la puesta en marcha de funciones de gestión de proyectos, que darán soporte al resto del proceso.

Algunas de las debilidades del modelo son:

- El Modelo CMMI puede llegar a ser excesivamente minucioso para algunas organizaciones sin proceso de desarrollo establecido.
- Puede ser considerado prescriptivo. Sin la adecuada consultoría para su aplicación, el modelo tiende a indicar las acciones que una organización debe realizar para alcanzar un nivel, sin una apropiada explicación de la metodología a aplicar.
- Requiere una gran inversión para ser completamente implementado. El modelo aplicado en su totalidad requiere de herramientas informáticas que asistan a la gestión de proyectos, y una plantilla de personal adecuada para lograr la gestión efectiva del proceso y su mantenimiento.
- Puede ser difícil de entender. Nuevamente, sin la adecuada consultoría, su interpretación y aplicación puede tornarse una tarea compleja.
- La mejora propuesta por el modelo no se encuentra directamente alineada a los objetivos de la organización. El modelo describe la forma de realizar la mejora, sin una adecuada guía del entorno empresarial necesario para su implementación.

La aplicación del modelo en PYMES [64] presenta dificultades manifiestas, como son:

- No existe una guía de la aplicación del modelo para pequeñas organizaciones. Inicialmente el Proceso de Mejora se dirigía a grandes corporaciones, con áreas dentro de las mismas dedicadas a temas de calidad. La aplicación del modelo resulta muchas veces intimidante para las pequeñas organizaciones.
- Crecimiento del número de áreas dentro de la organización, como así también las prácticas a aplicar, tiempo, recursos y un incremento en los costes hasta lograr resultados
- El Retorno de la inversión (ROI) no ha sido validado aún en CMMI.
- CMMI es demasiado normativo, en especial con pequeñas organizaciones que, además, funcionan y evolucionan de distinta manera que las grandes.

- CMMI parece escrito para organizaciones ya maduras y vagamente escrito para ser usado en PyMES.

2.2.2 La Norma ISO/IEC 15504

La norma ISO/IEC 15504[10] proporciona un marco de trabajo para la evaluación de los procesos y establece los requisitos mínimos para realizar una evaluación de forma consistente. Actualmente esta norma está estructurada en siete partes como muestra la Figura 2. ISO/IEC 15504-7 define un marco de trabajo para determinar la madurez de la organización, de esta forma, se incorpora la posibilidad de evaluar a las organizaciones

ISO/IEC 15504 se organiza por niveles de madurez, dando así una "puntuación" a la organización y no sólo a nivel de proceso. El modelo de procesos de referencia que utiliza ISO/IEC 15504-7, propio de la industria del software, es la norma ISO/IEC 12207.

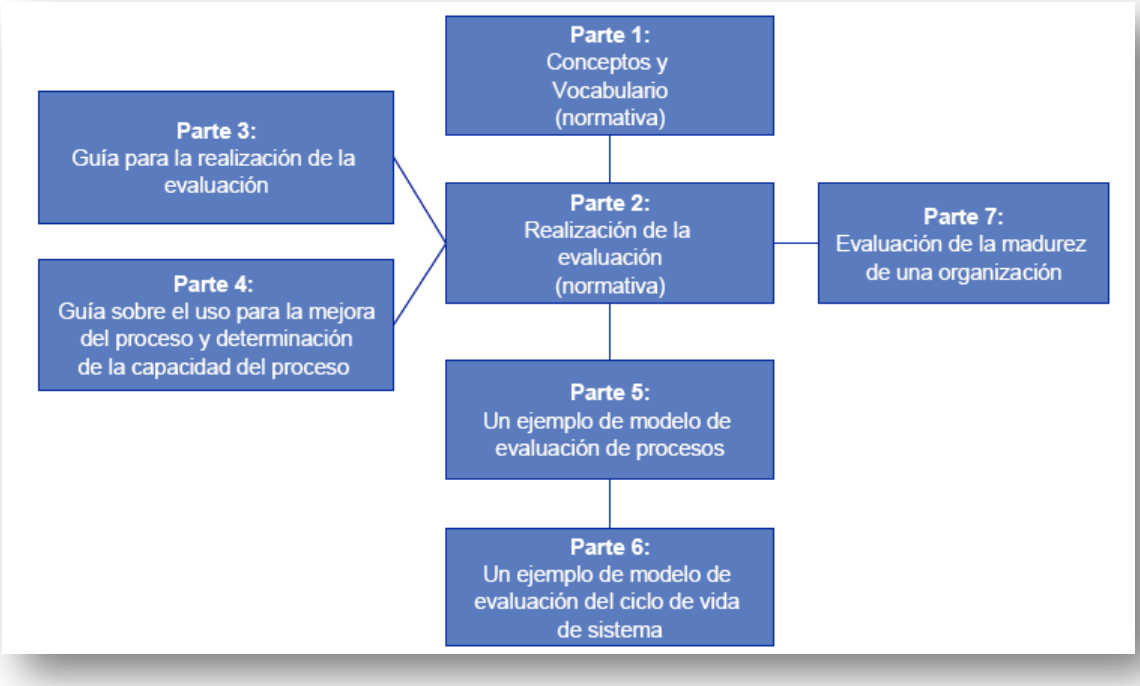


Figura 2. Estructura de la Norma ISO/IEC 15504

[10] http://www.iso15504.es/

La norma ISO/IEC 15504-7 establece 6 niveles de madurez para clasificar a las organizaciones, tal y como se muestra en la Figura 3.

Para que una organización pueda alcanzar un nivel de madurez debe evaluarse frente a la norma ISO/IEC 15504. Existen 3 clases de evaluaciones, clase 1, clase 2 y clase 3. Estas dos últimas se corresponden con evaluaciones internas y no ofrecen una certificación oficial, a diferencia de la clase 1 que es una evaluación más exhaustiva y rigurosa que permite alcanzar una puntuación oficial. En España, AENOR[11] ofrece este tipo de evaluaciónes y certificaciones bajo esta norma. Para realizar la evaluación se determina el nivel de capacidad de cada uno de los procesos, y una vez obtenidos derivarán en el nivel de madurez, de acuerdo a unas reglas de derivación establecidas en la norma.

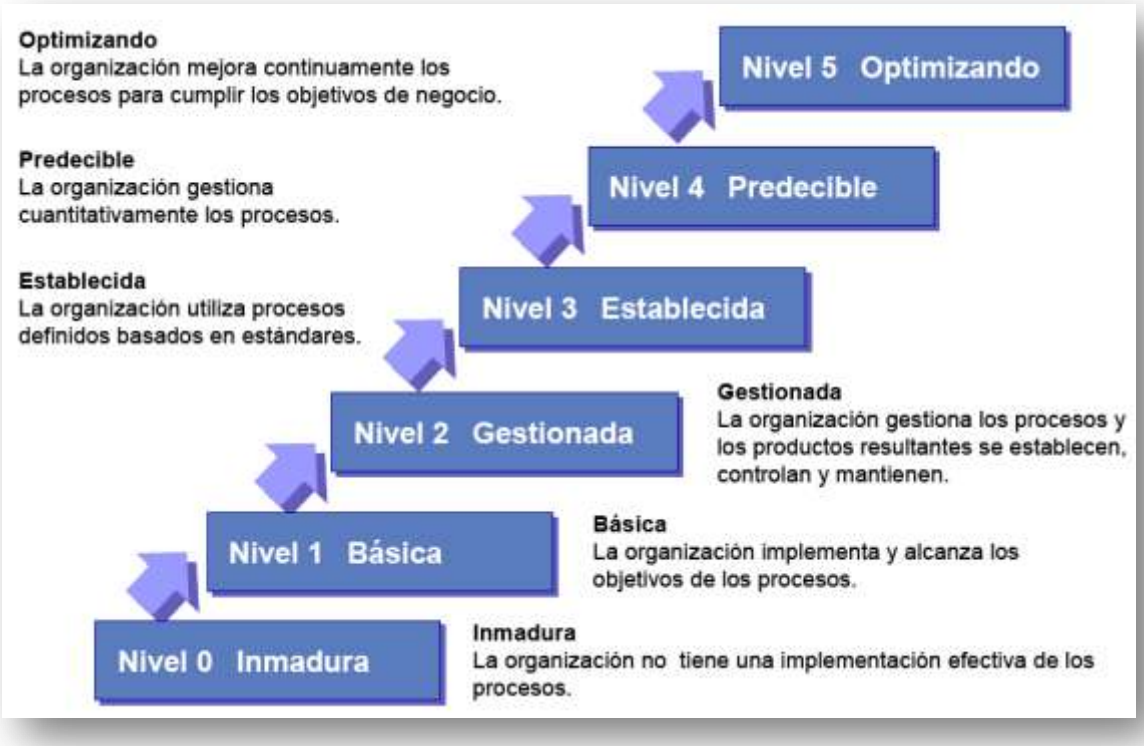


Figura 3. Niveles de Madurez de ISO/IEC 15504-7

[11] www.aenor.es/

2.2.3 Mejora en la Pequeña y Mediana Industria: El Modelo CompetiSoft

Las Pequeña y Mediana Industria (PyME) del Software compite actualmente con grandes organizaciones dedicadas al análisis y desarrollo de soluciones informáticas. En este contexto, las PyMEs se encuentran muchas veces en desventaja frente a sus competidores, debido a su inexperiencia o dificultad de adaptar su actividad a los estándares de calidad requeridos por el mercado.

Desde el punto de vista económico, la implementación de un proceso de mejora en organizaciones en crecimiento se ve dificultado por los altos costos de la asesoría y el tiempo que demanda esta actividad. A su vez, los modelos y estándares de mejora de procesos existentes (CMM, ISO) presentan una estructura organizacional compleja, y el retorno de la inversión esperado de su aplicación debe ser visto desde una perspectiva a largo plazo.

Respecto al soporte para la implantación de los procesos de mejora, la dedicación del personal y la documentación necesaria se ve sujeta a plazos y presupuestos escasos, razón por la cual muchas veces es relegada a favor de nuevos requerimientos o nuevos desarrollos. En consecuencia, el éxito de la implantación del proceso se encuentra asociado a las personas involucradas, convirtiendo esta actividad en un arte y no una ciencia.

Respecto a la capacitación del personal, las prácticas inherentes a la aplicación de modelos o estándares de calidad no son conocidas por el personal. La capacitación universitaria muchas veces transita estos temas en su modelo teórico, sin detenerse en la práctica. El personal abocado a la tarea de implantar un Modelo de Calidad específico debe ser debidamente formado y actualizado con las últimas prácticas aplicables a la industria. Cabe destacar que la oferta de capacitación en este particular no abunda en nuestro país.

El modelo de procesos CompetiSoft [53] es un modelo de calidad dirigido a las pequeñas y medianas organizaciones de Desarrollo de software, que tiene como fin estandarizar sus operaciones a través de la introducción de las mejores prácticas, alcanzando niveles internacionales en capacidad de procesos. Dicho modelo, al igual que ISO 15504 y CMMI, permiten a las organizaciones de desarrollo de software implementar las mejores prácticas en gestión, soporte e ingeniería con el fin lograr un valor agregado en sus procesos y entregar productos o servicios de calidad. El modelo fue desarrollado por un grupo de especialistas en calidad integrado por más de 100 investigadores de 24 entidades y 13 países de ambos lados del Atlántico, bajo la dirección de la Dra. Hanna Oktaba, siendo el resultado del proyecto de mejora de procesos para fomentar la competitividad de la pequeña y mediana industria del software de Iberoamérica, financiado por CyTED (Programa Iberoamericano de Ciencia y Tecnología para el desarrollo)[12].

El proyecto CompetiSoft se planteó como objetivo general incrementar el nivel de competitividad de las PyMES Iberoamericanas productoras de software mediante la creación y difusión de un marco metodológico común que, ajustado a sus necesidades específicas, pueda llegar a ser la base sobre la que establecer un mecanismo de evaluación y certificación de la industria del software reconocido en toda Iberoamérica.

El alcance se circunscribió a las empresas o áreas internas dedicadas al desarrollo y/o mantenimiento de software.

Las organizaciones, que no cuentan con procesos establecidos, pueden usar el modelo ajustándolo de acuerdo a sus necesidades; mientras que las organizaciones, que ya tienen procesos establecidos, pueden usarlo como punto de referencia para identificar los elementos que les hace falta cubrir.

Para la elaboración de CompetiSoft, fueron aplicados los siguientes criterios:

1. Generar una estructura de los procesos que esté acorde con la estructura de las organizaciones de la industria de software (Alta Dirección, Gestión y Operación).

[12] www.cyted.org/

2. Destacar el papel de la Alta Dirección en la planificación estratégica, su revisión y mejora continua como el promotor del buen funcionamiento de la organización.
3. Considerar a la Gestión como proveedor de recursos, procesos y proyectos, así como responsable de vigilar el cumplimiento de los objetivos estratégicos de la organización.
4. Considerar a la Operación como ejecutor de los proyectos de desarrollo y mantenimiento de software.
5. Integrar de manera clara y consistente los elementos indispensables para la definición de procesos y relaciones entre ellos.
6. Integrar los elementos para la administración de proyectos en un sólo proceso.
7. Integrar los elementos para la ingeniería de productos de software en un solo marco que incluya los procesos de soporte (verificación, validación, documentación y control de configuración).
8. Destacar la importancia de la gestión de recursos, en particular los que componen la base de conocimiento de la organización tales como: productos generados por proyectos, datos de los proyectos, incluyendo las mediciones, documentación de procesos y los datos recaudados a partir de su uso y lecciones aprendidas.
9. Basar el modelo de procesos en ISO9000:2000 y nivel 2 y 3 de CMM® V.1.1. Usar como marco general ISO/IEC 15504 - Software Process Assesment e incorporar las mejores prácticas de otros modelos de referencia tales como PMBOK[13], SWEBOK[14] y otros más especializados.
10. Crear un método de para evaluar los procesos software del modelo de procesos.

[13] www.pmi.org/PMBOK-Guide-and-Standards.aspx

[14] www.swebok.org/

11. Basar el modelo de evaluación en los principios de las normas internacionales ISO/IEC 15504-2: Performing an assesment e ISO/IEC 15504-4: Guiance on performing.
12. La prioridad más alta es satisfacer las necesidades de mejora es a través de la entrega temprana y continua de mejoras significativas al proceso de desarrollo y entregar con frecuencia mejoras del proceso de software (desde 2 hasta 6 meses)
13. No hay requisitos de mejora totalmente estables por parte de la organización. por ello, el diagnóstico es una actividad continua. Aún así, requisitos de mejora que surjan deberán ser priorizados y acogidos en la medida en que sea factible realizarlos.
14. Construir proyectos en torno a individuos motivados hacia la mejora de procesos individuales, grupales y organizacionales. Darles la oportunidad y el respaldo que necesitan y procurarles confianza para que realicen las tareas.
15. Promover el desarrollo sostenido. El trabajo deberá ser continuo e indefinido. La madurez del proceso, como el desempeño promedio de los proyectos, debe ser la medida primaria y liviana de la mejora del progreso. Las mediciones base para medir el desempeño son la productividad y la calidad.
16. Promover el aprendizaje continuo como una disciplina clave. El objetivo de esta disciplina es que permita conocer el trabajo, reflexionar acerca de éste y ajustar el trabajo a través de iteraciones cortas y concisas.

Considerando que este trabajo de tesis fue desarrollado en el marco del proyecto CompetiSoft, (modelo aplicado a nuestro caso de estudio) a continuación describimos sus características más detalladamente.

2.2.3.1 CompetiSoft: Un Enfoque Basado en Procesos

El modelo CompetiSoft está enfocado en procesos y considera los tres niveles básicos de la estructura de una organización que son: la Alta Dirección, Gestión y Operación. El modelo pretende apoyar a las organizaciones en la estandarización de sus prácticas, en la evaluación de su efectividad y en la integración de la mejora continua.

El modelo de procesos de CompetiSoft tiene tres categorías de procesos: Alta Dirección, Gerencia y Operación (Figura 4) que reflejan la estructura de una organización.

- La categoría de Alta Dirección contiene el proceso de Gestión de Negocio.
- La categoría de Gerencia está integrada por los procesos de Gestión de Procesos, Gestión de Proyectos y Gestión de Recursos. Éste último está constituido por los subprocesos de Gestión de Recursos Humanos, Gestión de Bienes, Servicios e Infraestructura y Gestión de Conocimiento.
- La categoría de Operación está integrada por los procesos de Administración de Proyectos Específicos y de Desarrollo y Mantenimiento de Software.

En cada proceso están definidos los roles responsables por la ejecución de las prácticas. Los roles se asignan al personal de la organización de acuerdo a sus habilidades y capacitación para desempeñarlos.

En CompetiSoft se clasifican los roles en Grupo Directivo, Responsable de Proceso y otros roles involucrados. Además se considera al Cliente y al Usuario como roles externos a la organización.

Los diez procesos definidos en el modelo CompetiSoft se incluyen dentro de tres categorías:

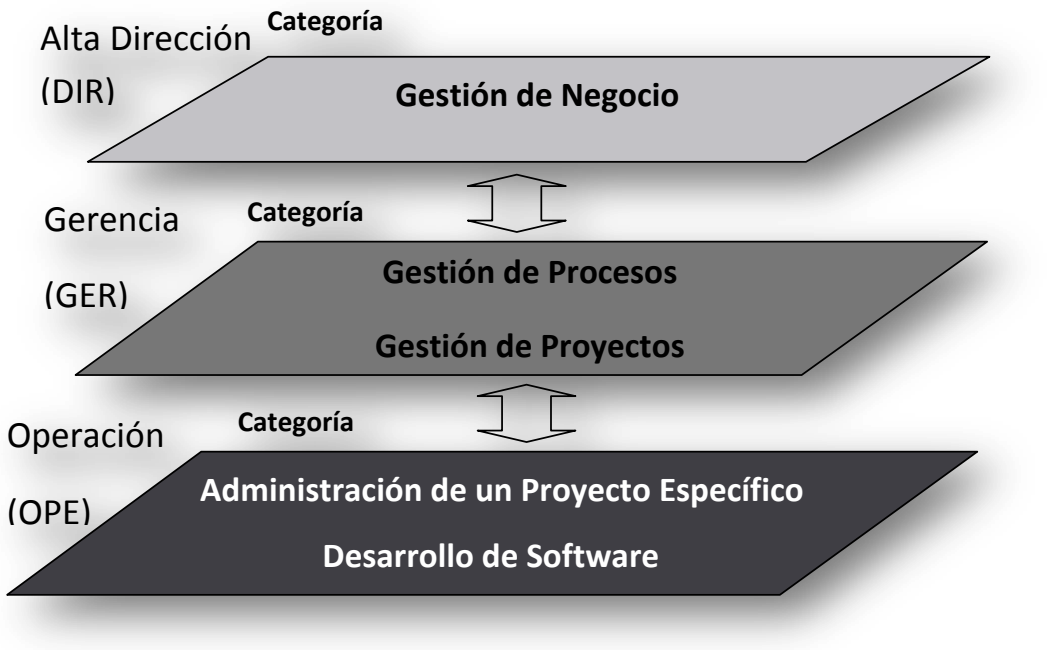


Figura 4. Estructura de Procesos del Modelo CompetiSoft

Categoría de Alta Dirección (DIR): Categoría de procesos que aborda las prácticas de Alta Dirección relacionadas con la gestión del negocio. Proporciona los lineamientos a los procesos de la Categoría de Gerencia y se retroalimenta con la información generada por ellos.

Categoría de Gerencia (GER): Categoría de procesos que aborda las prácticas de gestión de procesos, proyectos y recursos en función de los lineamientos establecidos en la Categoría de Alta Dirección. Proporciona los elementos para el funcionamiento de los procesos de la Categoría de Operación, recibe y evalúa la información generada por éstos y comunica los resultados a la Categoría de Alta Dirección.

Categoría de Operación (OPE): Categoría de procesos que aborda las prácticas de los proyectos de desarrollo y de mantenimiento de software. Esta categoría realiza las actividades de acuerdo a los elementos proporcionados por la Categoría de Gerencia y entrega a ésta la información y productos generados.

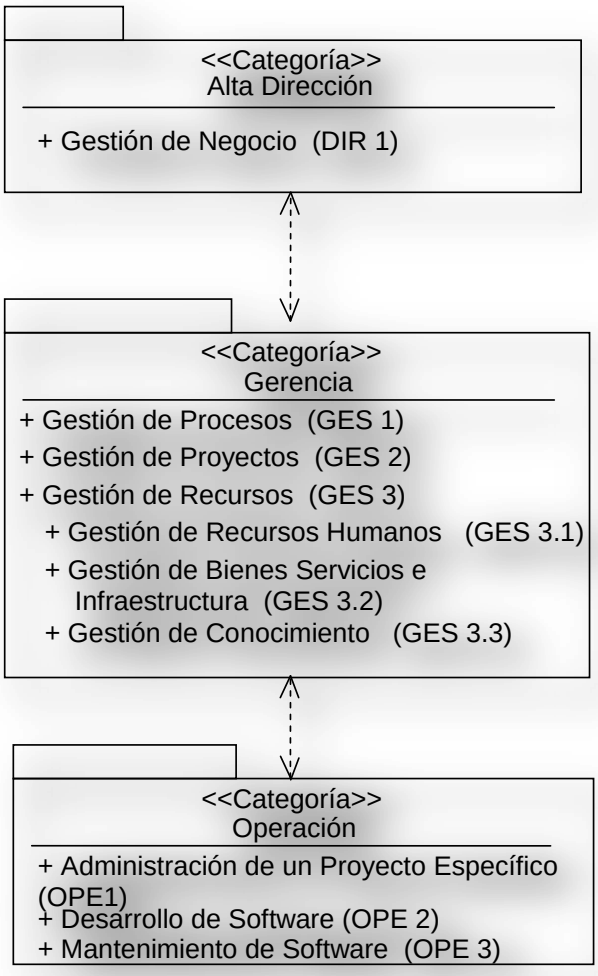


Figura 5. Diagrama de Categorías de Procesos

A continuación se listan los procesos definidos por el modelo de procesos (Figura 5):

1. DIR.1 Gestión de Negocio: El propósito de Gestión de Negocio es establecer la razón de ser de la organización, sus objetivos y las condiciones para lograrlos, para lo cual es necesario considerar las necesidades de los clientes, así como evaluar los resultados para poder proponer cambios que permitan la mejora continua. Adicionalmente habilita a la organización para responder a un ambiente de cambio y a sus miembros para trabajar en función de los objetivos establecidos.

2. GES.1 Gestión de Procesos: El propósito de Gestión de Procesos es establecer los procesos de la organización, en función de los procesos requeridos identificados en el plan estratégico. Así como definir, planificar, e implantar las actividades de mejora en los mismos.
3. GES.2 Gestión de Proyectos: El propósito de la Gestión de Proyectos es asegurar que los proyectos contribuyan al cumplimiento de los objetivos y estrategias de la organización.
4. GES.3 Gestión de Recursos: El propósito de Gestión de Recursos es conseguir y dotar a la organización de los recursos humanos, infraestructura, ambiente de trabajo y proveedores, así como crear y mantener la base de conocimiento de la organización. La finalidad es apoyar el cumplimiento de los objetivos del plan estratégico de la organización.
5. GES.3.1 Gestión de Recursos Humanos: El propósito de Gestión de Recursos Humanos es proporcionar los recursos humanos adecuados para cumplir las responsabilidades asignadas a los roles dentro de la organización, así como la evaluación del ambiente de trabajo.
6. GES.3.2 Gestión de Bienes, Servicios e Infraestructura: El propósito de Gestión de Bienes, Servicios e Infraestructura es proporcionar proveedores de bienes, servicios e infraestructura que satisfagan los requisitos de adquisición de los procesos y proyectos.
7. GES.3.3 Gestión de Conocimiento: El propósito de Gestión de Conocimiento es mantener disponible y administrar la base de conocimiento que contiene la información y los productos generados por la organización.

8. OPE.1 Administración de un Proyecto Específico: El propósito de la Administración de un Proyecto Específico es establecer y llevar a cabo sistemáticamente las actividades que permitan cumplir con los objetivos de un proyecto en tiempo y costo esperados.
9. OPE.2 Desarrollo de Software: El propósito de Desarrollo de Software es la realización sistemática de las actividades de análisis, diseño, construcción,

integración y pruebas de productos de software nuevos cumpliendo con los requerimientos especificados.

10. OPE.3 Mantenimiento de Software: El propósito de Mantenimiento de Software es la realización sistemática de las actividades necesarias para modificar productos software y adaptarlos a los nuevos requisitos y necesidades del producto.

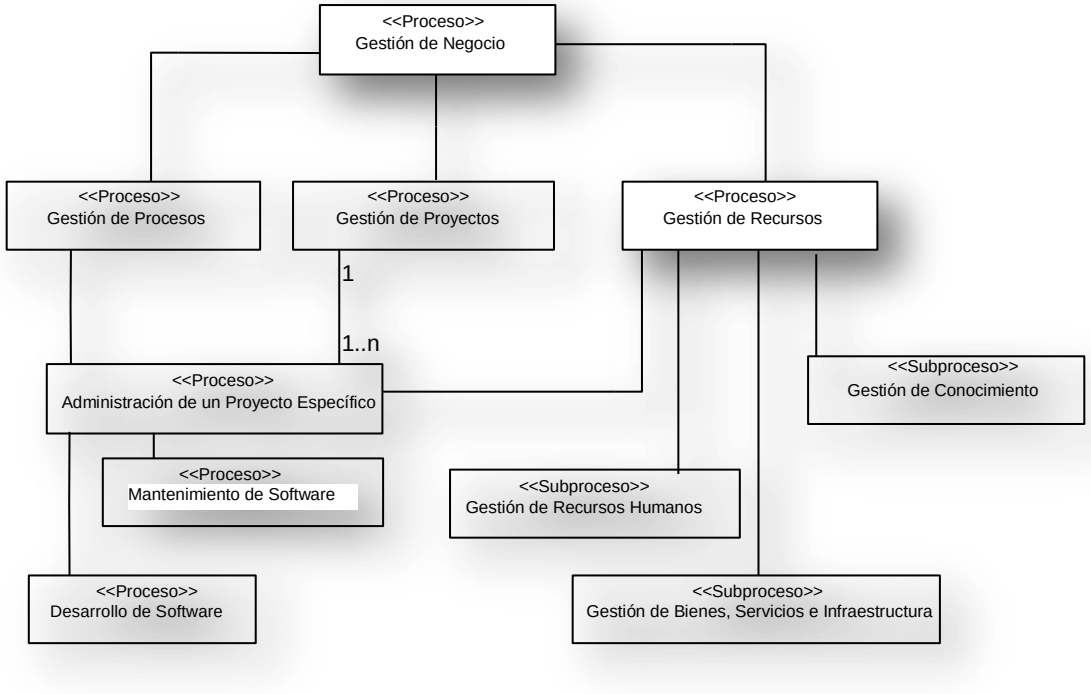


Figura 6. Diagrama de Relaciones entre Procesos

A nivel macro se establece la gestión de negocio como proceso rector de la organización, en donde se encontrará la aplicación de las estrategias organizacionales. A partir de allí surgen tres procesos claramente identificables (Figura 6): (1) Todo lo relacionado con diseño y formalización de procesos en general; (2) Planificación y ejecución de proyectos; y (3) Definición y planificación de recursos.

El modelo CompetiSoft define roles según las competencias, como podemos observar en la Figura 7:

1. Cliente: Es el que solicita un producto de software y financia el proyecto para su desarrollo o mantenimiento.
2. Usuario: Es el que va a utilizar el producto de software.
3. Grupo Directivo: Son los que dirigen a una organización y son responsables por su funcionamiento exitoso.
4. Responsable de Proceso: Es el encargado de la realización de las prácticas de un proceso y del cumplimiento de sus objetivos.
5. Involucrado: Otros roles con habilidades requeridas para la ejecución de actividades o tareas específicas. Por ejemplo: Analista, Programador, Revisor, entre otros.

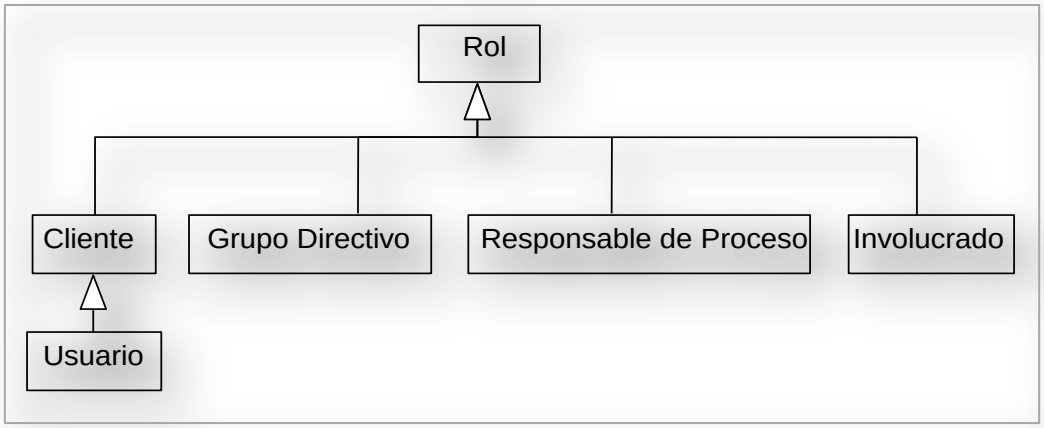


Figura 7. Clasificación General de Roles

2.3 Contribuciones de la Mejora de Procesos al Gobierno Electrónico

En algunas ocasiones relacionadas con otros beneficios, como eficiencia y calidad en el servicio, se considera que las tecnologías de información y comunicación pueden inducir profundos cambios en las estructuras gubernamentales existentes. Por ejemplo,

algunos autores comentan que debido a las capacidades de Internet y las tecnologías de red, se espera que las organizaciones se vuelvan más flexibles y horizontales; en contraste con las organizaciones burocráticas existentes que son altamente jerárquicas y formalizadas [31]. Sin embargo, investigación reciente ha encontrado que los efectos de las tecnologías de información y comunicación en las estructuras organizacionales del gobierno no son tan significativos como se esperaba [38]. De forma adicional, otros estudios argumentan que el hecho de que se den o no cambios estructurales, así como otro tipo de cambios, derivados del uso de tecnologías de información en el gobierno, está en función de los intereses de quienes impulsaron la iniciativa, pues uno de los principales factores a considerar es si el sistema redistribuye el poder en la organización o mantiene las estructuras de autoridad prevalecientes [30][46].

La capacidad de las tecnologías de información y comunicación para generar los beneficios mencionados dependen, al menos de forma parcial, de la existencia de ciertos factores o requisitos [36]. Estos factores tecnológicos, gerenciales y de política pública tienen un importante impacto tanto en la calidad de las iniciativas de gobierno electrónico como en los beneficios obtenidos por los gobiernos, ciudadanos y otros grupos de interés [3].

El insumo primordial de cualquier sistema de información gubernamental es precisamente la información o datos existentes. La calidad de las estructuras y definiciones de estos datos tiene una gran influencia en el tipo de sistema que se puede desarrollar [1][19]. Esta calidad se puede evaluar tomando en consideración qué tan exacta, completa y consistente es la información [53]. Los efectos de tener información de baja calidad se ven reflejados en la poca utilidad de las misma para apoyar procesos y decisiones al interior de la organización, así como para realizar reportes y evaluar impactos ante entidades externas [44]. En el caso específico de desarrollo de sistemas de información, uno de los principales costos en procesos de integración o desarrollo de sistemas para el soporte a las decisiones está en la limpieza y acondicionamiento de los datos [21][24].

Un determinante importante en proyectos de gobierno electrónico es la disponibilidad de infraestructura tecnológica adecuada. Dos de las principales características de la tecnología que impactan su éxito es su utilidad para los objetivos concretos de la organización y el grado de dificultad que presenta para los usuarios [18][50]. En algunos casos existe la tecnología necesaria, pero ésta no es necesariamente compatible entre departamentos o dependencias gubernamentales lo que limita la utilidad y éxito del proyecto [11][19]. Otro factor de gran relevancia es la disponibilidad de recursos humanos con los conocimientos y las habilidades tecnológicas necesarias [14][21].

Como en muchos otros proyectos que involucran cambio organizacional, ciertas características de la estructura organizacional o del estilo gerencial son importantes factores de éxito o fracaso para iniciativas de gobierno electrónico. Algunos de los factores identificados en los estudios existentes son el tamaño del proyecto, la diversidad de usuarios, la resistencia al cambio y la compatibilidad entre los objetivos del proyecto y las metas organizacionales [7][9][21][27][43]. Por otro lado, en el caso de iniciativas que involucran la participación de varias dependencias, existen otros factores que deben ser considerados: la heterogeneidad de las organizaciones involucradas, la complementariedad o grado de conflicto existente entre sus metas y tensiones de poder entre las distintas organizaciones [14][20][21][56].

Considerando entonces, que el e-gov busca redefinir la relación entre los ciudadanos y el estado, esta relación que puede definirse como un sevicio debería cumplir con ciertas características de disponibilidad, accesibilidad y contenido de manera tal que el ciudadano se convierta en un “usuario” de dicho servicio. Cuando empezamos a definir características deseables del servicio comenzamos a transitar un camino que indefectiblemente nos llevará a establecer la calidad deseada, la cual deberemos medir, es aquí entonces donde resultaría conveniente la utilización de un estándar de calidad como los expuestos precedentemente, para asegurar que el producto que se construya, como mostraremos en el Capítulo siguiente, contenga esos aspectos deseables que faciliten la relación entre ciudadanos y el estado.

3 MEJORA DE PROCESOS COMO SOPORTE AL GOBIERNO ELECTRÓNICO: GUÍAS Y LECCIONES DESDE EL CASO DE ESTUDIO

Los cinco niveles de evolución de gobierno electrónico, según un estudio de las Naciones Unidas [28] se definen de la siguiente manera:

> 1 – Presencia Emergente: La presencia del gobierno incluye una página web y/o un sitio web oficial, con información limitada, básica y estática; enlaces para los ministerios / departamentos de educación, salud, bienestar social, trabajo y finanzas pueden o no existir; enlaces para gobiernos locales / regionales pueden o no existir; alguna información almacenada, como un mensaje del jefe de estado o un documento como la Constitución puede estar disponible en línea; la mayor parte de la información permanece estática, con pocas opciones para los ciudadanos.
>
> 2 – Presencia mejorada: El gobierno provee información sobre políticas públicas, leyes, normas, informes, noticias y archivos para ser descargados por el usuario. Incluye las características del Portal emergente, complementado con opciones de interactividad, servicio al cliente y enlaces; calidad optimizada y creciente cantidad de información; la información brindada es actualizada con mayor regularidad.
>
> 3 – Presencia interactiva: Interacción en las dos direcciones con servicios en línea para mejor conveniencia del usuario, como obtención de formularios para pago de tarifas e impuestos o para la renovación de licencias; bases de datos accesibles y personalizadas; comunicación extensiva por correo electrónico interna y externamente; el sitio es actualizado constantemente para mantener la información actualizada para el público.
>
> 4- Presencia transaccional: Posibilita transacciones completas entre el gobierno y el ciudadano – "pleno tratamiento electrónico de casos"; los usuarios pueden pagar los servicios, tarifas o impuestos y realizar transacciones financieras en

línea, obtener tarjetas de identificación, partidas de nacimiento, pasaportes, renovación de licencias y otras especies de interacciones, en una base en línea 24h/7días; suministro de bienes y servicios están habilitados para licitación en línea.

5 – Presencia sin discontinuidad: gobierno plenamente en red con todas las agencias interconectadas; participación ciudadana en los procesos de diálogo, consultas y toma de decisiones; cooperación e integración con el sector privado y la sociedad organizada.

En la implementación de e-gov pueden distinguirse tres capas necesarias [29] para que los servicios sean alcanzados por los ciudadanos:

- Hay una primer capa de infraestructura en (tele)-comunicaciones, que puede ser física o inalámbrica. Resulta indispensable que esta infraestructura provea a los ciudadanos del acceso a la internet global para que éstos puedan utilizar los servicios de e-gov.
- La segunda capa está compuesta por las soluciones de software y plataformas. De hecho entre internet y los e-services existen numerosas soluciones de software como por ejemplo plataformas de repositorio de datos, plataformas de gestión de datos, plataformas de publicación, etc. Estas, por lo general están desarrolladas por empresas privadas.
- La tercera capa esta compuesta por los servicios de e-gov, los cuales son ofrecidos por distintas agencias del estado para los ciudadanos.

Es importante hacer esta distinción de las tres capas, porque el rol del estado es diferente en cada una de ellas. Es muy común que el ciudadano sólo asocia e-gov con la tercer capa, pero las tres capas son necesarias para comprender una política de e-gov o e-política. Veamos entonces cual es el rol del estado en cada una. Respecto a la primera, la de servicios de (tele)-comunicaciones que provee el acceso a la internet global, existe un consenso generalizado respecto que la necesidad de que los ciudadanos puedan acceder a la internet global debe formar parte de cualquier política de e-gov. Si bien en

muchos casos este servicio es brindado por empresas privadas, no debe escapar al estado generar las condiciones para que ello suceda como así también el de regular el negocio definiéndolo como una Obligación de Servicio Universal en términos de accesibilidad, calidad y asequibilidad (para reducir la llamada brecha digital).

3.1 Programa de e-gov en el Poder Judicial de la Provincia de Neuquén

En el año 1997, el Poder Judicial de la Provincia de Neuquén (PJN) inicia la transformación cultural de su manera de trabajo con la incorporación de la tecnología informática.

En el proyecto de informatización de ese entonces existían defectos producto de no tener en el país antecedentes ni experiencias similares que buscaran abarcar la totalidad del trámite judicial ni la totalidad de organismos. Esas carencias de origen fueron saneadas con la firme decisión política de llevar a buen puerto el proyecto, dotándolo de los recursos materiales y humanos necesarios. Es importante resaltar el esfuerzo puesto de manifiesto en los Magistrados, Funcionarios y Empleados que colaboraron para construir en conjunto con el organismo encargado del proyecto, la Secretaría de Informática. Esta ha sido una condición necesaria para construir con bases sólidas una nueva cultura de trabajo organizacional.

Hoy podemos decir que el gran paso de la transformación de la cultura del trabajo se ha dado en esta organización, porque la herramienta informática es parte de la vida diaria de los organismos. En esto la capacitación de todo el personal ha jugado un rol preponderante.

La principal motivación de un sistema que registra información es pensar en todo lo que seremos capaces de hacer cuando tengamos la información disponible en el momento que la necesitemos y de la forma que la necesitemos. Esta motivación, en muchos casos lleva, erróneamente, a preocuparse por cuestiones superficiales de información que

mostrar, listar o graficar sin tener en cuenta cómo se obtiene esa información. La Secretaría de Informática (SI) siempre ha postulado que informatizar la gestión significa incorporar una herramienta tecnológica al trabajo diario de los organismos jurisdiccionales. Dicho trabajo se realiza con la asistencia de las herramientas tecnológicas en donde el registro de la información es una consecuencia de la tarea realizada. En tal sentido se ha puesto el énfasis en los siguientes puntos:

- Se debe definir la estructura organizacional y recursos necesarios para implementar y mantener tecnologías.
- Cada agente productor de documentos debe contar con una estación de trabajo.
- La gestión debe abarcar desde la mesa de entradas hasta la sentencia.
- Las actuaciones que se realicen durante la gestión del expediente, deben generarse y preservarse en formato electrónico.

De esta manera, sin olvidarse de que la información que se registre será utilizada posteriormente con fines estadísticos y de control de gestión, el foco principal estuvo en proveer las bases necesarias para un registro seguro y consistente de la información, convirtiéndose las bases de datos en el mayor capital informático de la organización.

Se ha construido entones, una plataforma de base que permite pensar en brindar mayores servicios al ciudadano a partir de la disponibilidad de información en formato electrónico, citando como ejemplo: Sistema de publicación de listas de despacho en Internet; Consulta personalizada de expedientes (procuración electrónica); Lista de distribución de providencias a los correos electrónicos de los patrocinantes; Publicación del texto de las providencias en Internet; Publicación de jurisprudencia internet; y Registro Único de Adoptantes.

Es importante destacar que el desembarco de soluciones tecnológicas en una organización tradicional como el Poder Judicial, genera diversas incertidumbres entre los empleados, y la certeza de que habrá cosas que cambiarán, que el trabajo habitual cambiará con la presencia del nuevo sistema y que los empleados deberán hacer su

trabajo de una manera diferente. Es aquí donde comienza el problema de la resistencia al cambio: las personas se sienten seguras porque conocen cómo hacer su trabajo, lo tienen incorporado en el subconsciente, pero con la llegada del nuevo sistema no saben cómo deberán hacerlo y en algunos casos desconocen si serán capaces de hacerlo o no desean hacer el esfuerzo de aprender. Para comprender mejor éste fenómeno repasemos brevemente cuales son los pasos en el proceso de aprendizaje por el que pasan los actores (Figura 8):

- Estado Inicial: La persona es incompetente en una disciplina o tema y no tiene siquiera conciencia de su incompetencia.
- Primer escalón: cuando toma conciencia de su incompetencia, sólo tiene el conocimiento de la existencia de dicha disciplina y una idea sobre ella.
- Segundo escalón: poniendo gran esfuerzo y atención a los detalles logra pasar al nivel en que es conscientemente competente, comprende la disciplina y la comienza a aplicar con gran dedicación.
- Tercer escalón: luego de mucha práctica sobreviene, el estado de ser competente desde el subconsciente. Ya no es necesario aplicar tanta atención, ahora sí se puede decir que ha aprendido.

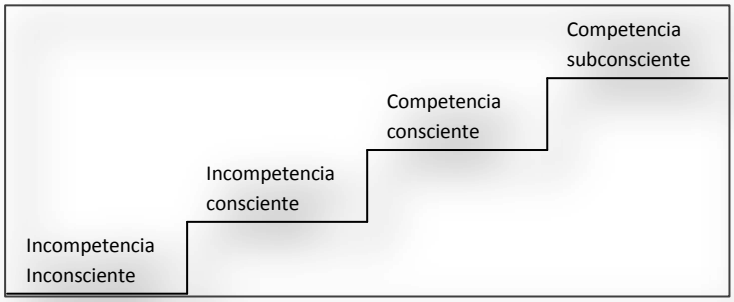


Figura 8. Proceso de Aprendizaje

Para ilustrar este proceso, recordaremos los esfuerzos para aprender a andar en bicicleta, a manejar un automóvil o a practicar un nuevo deporte. Durante el aprendizaje el ser humano va internalizando la complejidad de detalles en su subconsciente (buen

manejador de la complejidad de detalles), dejando la faz consciente libre para determinar el rumbo. Ahora podemos disfrutar del paseo en bicicleta y elegir a dónde vamos.

En el proceso de informatización de una organización ocurre algo parecido. Se definen, lenta y trabajosamente la complejidad de detalle de sus procesos, para luego ser internalizados en su subconsciente (sistema de software), quien deberá manejar esa complejidad de detalles. De este modo, la Secretaría de Informática conjuntamente con la Escuela de Capacitación planificó y ejecutó una capacitación cuyo objetivo fue poner al usuario en el escalón de la "competencia consciente" respecto a la nueva forma de hacer su trabajo, para que luego de un entrenamiento asistido en el uso diario se pasara a la "competencia subconsciente".

El uso de un sistema informático de gestión desde el año 1997, ha producido, sin duda, una evolución y madurez en el uso de herramientas tecnológicas para "apalancar" el trabajo que antes se hacía manualmente. Pero en la Secretaría de Informática siempre ha estado el espíritu de mejora, que la organización ha acompañado; es por esto que luego de madurar el cambio con la informatización del 100% de los organismos jurisdiccionales, se ha planificado una nueva iteración de mejora incorporando nuevas tecnologías para el tratamiento de documentos con capacidad de firma electrónica, utilizadas exitosamente en la Justicia de España, Canadá y Australia entre otras. De este modo la Secretaría de Informática ha trabajado y trabaja ejecutando lo planificado en los planes estratégicos 2005-2009 y 2010-2015.

Como se menciona en el Capítulo 1, la irrupción de las nuevas Tecnologías de la Información y las Comunicaciones (TICs) en las últimas décadas ha generado un notable impacto en la vida cotidiana de la sociedad, como medio de difusión y procesamiento de información. El Poder Judicial de Neuquén ha invertido años de trabajo y esfuerzo, cuidadosamente planificados, para lograr el cambio de la cultura organizacional, que fue condición necesaria para que hoy junto a los recursos tecnológicos sean la base de sustento de la publicación de información para actores internos y externos, estableciendo el marco adecuado para impulsar el uso intensivo de

estas nuevas tecnologías, a fin de optimizar así la gestión pública de manera permanente, con el propósito de ofrecer mejores servicios al ciudadano, facilitar trámites y reducir sus costos, generar nuevos espacios de participación, y reducir la "brecha digital" incluyendo a personas, empresas y comunidades menos favorecidas.

El rumbo adoptado es el que se encamina hacia el concepto de Gobierno Electrónico, enfocándose en el uso de las Tecnologías de Información y Comunicación (TICs) para redefinir la relación del gobierno con los ciudadanos, mejorar la gestión y los servicios, garantizar la transparencia y la participación y facilitar el acceso a la información pública, apoyando la integración y el desarrollo de los distintos sectores.

Para comenzar a transitar este camino se trabajó inicialmente en dos pilares estratégicos:

- La gestión de recursos para los proyectos.
- La definición y fortalecimiento de la estructura encargada de dar soporte al usuario.

Estos dos pilares permitieron sentar las bases para luego comenzar a pensar en prácticas de gobierno electrónico que sean sustentables y mantenibles en el tiempo, con el objeto de reemplazar en el futuro a los procesos manuales y de atención personalizada que se lleva adelante hoy en día.

3.1.1. Gestión de Recursos para los Proyectos

La Secretaría de Informática del Poder Judicial de Neuquén es un organismo dedicado a prestar servicios relacionados con el uso de la tecnología de información y comunicaciones, donde una de sus especialidades es asistir al usuario final en el uso de aplicaciones de software desarrolladas internamente o por terceros. En tal sentido la SI es un área de apoyatura técnica para los organismos jurisdiccionales que son quienes llevan adelante el proceso de justicia. Del el mismo modo que la SI, existen otros organismos como la Administración General, quien se ocupa de los recursos financieros y de adquisición de bienes y servicios.

La Figura 9, ilustra como se relacionan los organismos no jurisdiccionales (auxiliares de la justicia) y los jurisdiccionales quienes se encargan según su rol, de impartir justicia.

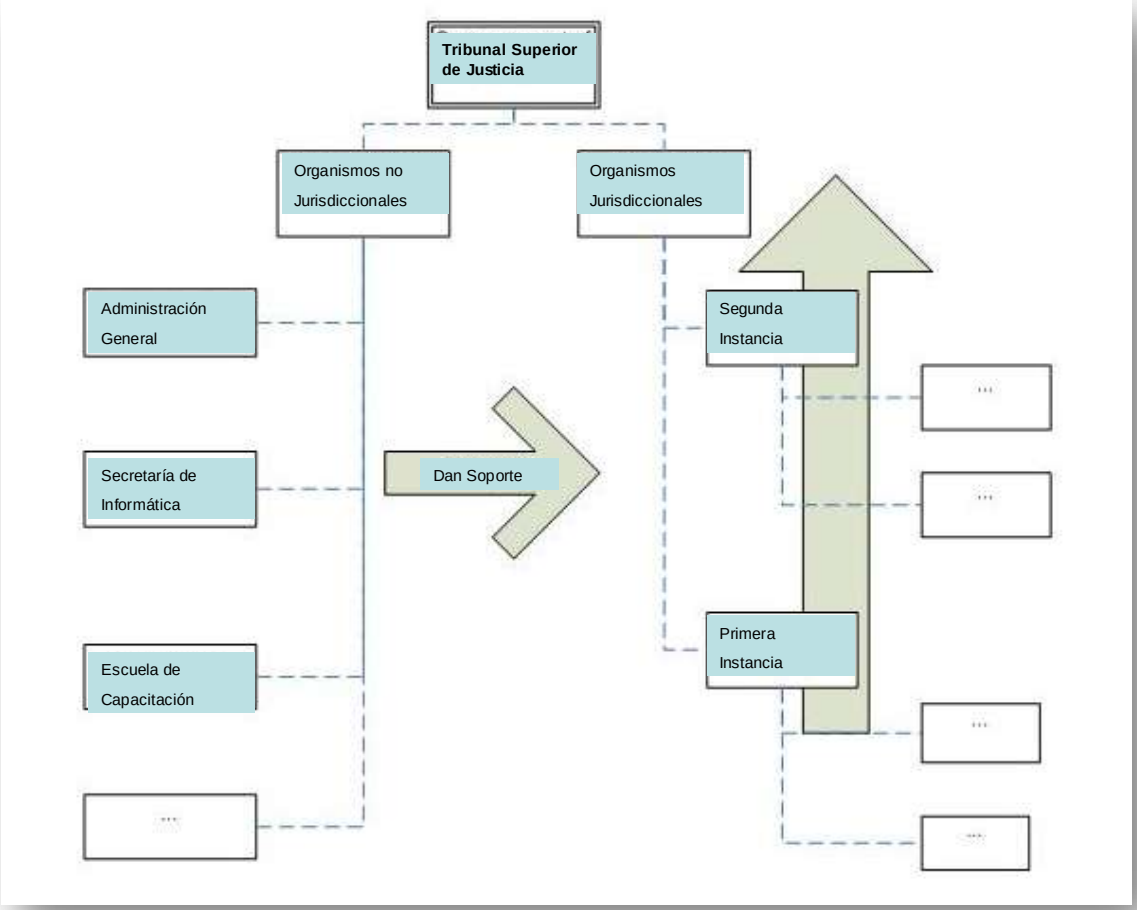


Figura 9. Relación entre Organismos Jurisdiccionales y Organismos Auxiliares de Justicia

La SI tiene delimitadas sus funciones dentro de la organización, quien la define como una unidad de gestión operativa cuya misión es brindar apoyo a los organismos judiciales, utilizando la tecnología informática como herramienta tendiente a mejorar la calidad del servicio de Justicia, estableciendo las siguientes funciones:

1. Supervisar y mantener operativos todos los sistemas utilizados en la gestión judicial, así como proponer las mejoras o reemplazos de los mismos cuando se estime conveniente.

2. Mantener la plataforma tecnológica de hardware existente, proponiendo las actualizaciones o reemplazos que se estimen convenientes.

3. Ejecutar el plan anual de proyectos informáticos.

4. Implementar las políticas informáticas que se definan conjuntamente con el Departamento de Planificación y Desarrollo.

5. Definir, documentar y ejecutar estándares y procedimientos tendientes a mejorar la gestión operativa del organismo.

6. Gestionar riesgos que amenacen a proyectos informáticos en ejecución y a sistemas utilizados en la gestión judicial.

7. Asesorar en materia informática al Administrador General.

8. Intervenir en el diseño y redacción de contratos informáticos en los que intervenga el Poder Judicial de Neuquén.

9. Intervenir en la redacción de pliegos para la adquisición de hardware y software.

10. Asesorar técnicamente a comisiones de preadjudicación de compra de equipamiento informático.

11. Recepcionar y poner en marcha del equipamiento informático que adquiera el Poder Judicial de Neuquén.

12. Distribuir los recursos informáticos, atendiendo a las necesidades que requiera cada organismo.

13. Implementar laboratorios de investigación informática a los efectos de brindar servicios específicos en el ámbito jurisdiccional.

Para ello se encuentra organizada en cuatro areas de especialidad, con funciones acordes a sus habilidades:

Area Infraestructura Tecnológica

1. Ejecución de las tareas de evaluación, medición, documentación y prevención, respecto de los sistemas de base puestos en producción.

2. Investigación, análisis, evaluación, prueba, documentación y definición de nuevas herramientas informáticas de base a incorporar en la Gestión Judicial.

3. Definición y actualización de estándares y procedimientos del uso de la tecnología existente y la que se adquiera en el futuro.

4. Puesta en marcha de la nueva tecnología informática que se adquiera, generando los estándares y procedimientos para su utilización.

5. Transferencia al Area Operaciones el mantenimiento de la tecnología implementada.

6. Soporte de segundo nivel a las demás áreas de la Secretaría que así lo requieran y no esté explicado en la documentación existente.

7. Definición, actualización e implementación de seguridad para la plataforma informática.

8. Creación y mantenimiento de un laboratorio de investigación y pruebas que permita a la a la Secretaría obtener mejores resultados en sus trabajos y así mejorar los servicios prestados por el organismo.

9. Mantenimiento del orden, prolijidad y documentación en todas las instalaciones de equipamiento que dependan del Area.

Area Operaciones

1. Administrar la tecnología informática utilizada en la Gestión Judicial.

2. Supervisar el cumplimiento de los estándares definidos y condiciones iniciales observadas.

3. Comunicar al Area Infraestructura Tecnológica aquellos problemas que no puedan ser solucionados en la plataforma tecnológica.

4. Mantener las aplicaciones y el software de base en uso procurando optimizar su rendimiento.

5. Documentar todos los procesos, procedimientos e instructivos que genere el Area por mejoras en el mantenimiento de los equipos y programas.
6. Relevar, analizar, diseñar e implementar una metodología de trabajo para los Operadores por Fuero.
7. Brindar soporte de primer y segundo nivel operativo a los usuarios de las dependencias judiciales.
8. Evaluar la calidad de atención a usuarios periódicamente.
9. Detectar necesidades de capacitación en los organismos judiciales, que permita reducir las necesidades de soporte técnico insitu.

Area Desarrollo

1. Realizar tareas de relevamiento, análisis, diseño y construcción de sistemas de software.
2. Respetar los estándares y metodología de trabajo definida en la Secretaría.
3. Evaluar la factibilidad de aplicar soluciones informáticas para mejorar el desempeño de los organismos judiciales.
4. Evaluar la metodología de trabajo con el objeto de mejorar el proceso de los futuros desarrollos.
5. Evaluar herramientas de desarrollo de software.
6. Capacitar al personal de la Secretaría en el uso de herramientas de desarrollo.
7. Intervenir proactivamente en la definición de estándares y procedimientos que afecten al área.
8. Participar en la implementación los sistemas construidos y en los casos que corresponda realizar la transición al mantenimiento al Area Operaciones.

9. Definir variables de medición del desempeño de los sistemas que se implementen, con el objeto de utilizar estas variables para el mantenimiento y la mejora continua de los sistemas desarrollados.

10. Supervisar ejecución de contratos informáticos, contratado con por el PJN.

Area Administración y Logística

1. Brindar soporte administrativo para mantener la documentación formal que deban generar el Secretario de Informática, las áreas: Operaciones, Infraestructura Tecnológica y Desarrollo.

2. Gestionar la documentación administrativa de la Secretaría de Informática, esto es: recibir, organizar, archivar y enviar todo tipo de documentos que formen parte de la gestión administrativa.

3. Concentrar todos los pedidos de equipamiento, tanto internos como externos a la Secretaría, con el objetivo de gestionar eficientemente la provisión de los mismos, según el mecanismo de compra que corresponda reglamentariamente.

4. Supervisar y ejecutar el traslado e instalación de los equipamientos informáticos para puestos de trabajo, procurando mantener el orden y prolijidad en dicha tarea.

5. Gestionar la reparación de equipamiento informático, manteniendo un registro detallado de los elementos a reparar.

6. Gestionar la baja de equipamiento cuando corresponda por razones de obsolescencia, falta de uso o imposibilidad de reparación.

7. Gestionar reclamos de garantía de equipamiento informático.

8. Mantener un registro detallado de las licencias de software existentes en el Poder Judicial.

9. Controlar y gestionar el stock de equipamiento, repuestos e insumos existentes en depósitos, manteniendo en todo momento registros actualizados.

10. Mantener registros actualizados del equipamiento informático instalado en el Poder Judicial.

11. Controlar y elaborar la rendición periódica del fondo permanente para gastos y viáticos.

Cada tarea de coordinación de actividades en las que el factor humano interviene para alcanzar los objetivos previamente definidos se debe realizar de una manera sistémica y de acuerdo con las buenas prácticas. De esta manera, una buena organización no sólo se caracteriza por la disposición de sus actividades, sino también por su gestión y control. Con estas declaraciones en mente, en 2005 el PJN ha elaborado el plan estratégico de la organización (2005-2010) (2011-2015), que define las directrices en donde claramente se detalla el nivel de importancia de la Informática dentro de la gestión de los procesos.

Previamente, antes de 2005, la SI sólo fue la encargada de una tarea: la aplicación de un sistema de software desarrollado por un tercero. Por ello, la disposición de las personas en las zonas era muy diferente en esos días. La organización se centraba en la aplicación de desarrollos de terceros, y toda la ayuda estaba dirigida a esta actividad. En consecuencia, no hubo "zona de desarrollo". Ahora, con base en el plan estratégico, y debido a un conjunto de metas y objetivos que tendían a la sustitución del sistema de software de gestión judicial, se han destinado recursos para la adopción de nuevas tecnologías y para mejorar la asistencia del usuario. El logro de estas metas y objetivos consistió en el desarrollo o la creación de áreas específicas de la SI, y por supuesto, el establecimiento de sus objetivos internos. Sobre la base de los diferentes objetivos, se diseñaron el alcance y las redes de información. La intención principal era mantener todos los procesos bajo control. La parte difícil fue tomar una decisión acerca de "qué

persona debe ser asignada a qué área", es decir, los recursos humanos tenidos en cuenta para obtener la mejor distribución.

Un buen punto de partida fue tratar de entender la motivación detrás de cada persona para llevar a cabo una actividad en particular - si él / ella se sentía satisfecho/a con su trabajo, cuáles eran las expectativas que él / ella tenía, y lo más importante, las relaciones humanas como equipo de trabajo. En este punto, la consigna era clara: había que organizar a la gente en un grupo capaz de lograr las metas y objetivos del plan estratégico. Este grupo de personas constituyen uno de los "recursos" con el que la SI debe contar para desarrollar el plan estratégico. En ese momento consideramos la posibilidad de usar un modelo de referencia para la gestión de recursos como un buen punto de partida. Esa fue nuestra conexión con los modelos de mejora de procesos software, y en particular con CompetiSoft.

3.1.1.1 Mejora en la Gestión de Recursos

Los principales objetivos de la gestión de recursos (RM) en CompetiSoft son proporcionar a la organización los recursos humanos, infraestructura, los registros de proveedores y la administración de la Base de Conocimientos de la organización. El objetivo principal de la zona de RM es apoyar las actividades hacia el logro de los objetivos del Plan Estratégico. Las principales actividades involucradas en el área de RM son las siguientes:

- Planificación de recursos: se recibe la información del Plan Estratégico y Plan de Formación de Adquisición, de los procesos y de los proyectos. Como resultado de esta actividad, se producen los siguientes planes: Plan Operativo de Recursos Humanos y Medio Ambiente de Trabajo, Plan Operativo de Productos Servicios, Infraestructura y Plan Operativo de Organización del Conocimiento.
- Seguimiento y control: se establece una visibilidad adecuada en un progreso real para que la dirección pueda tomar medidas eficaces en todos los sub-procesos al considerar la información de Recursos Humanos, Medio Ambiente, Bienes,

Servicios e Informe de Infraestructura, y del informe de situación respecto de la Organización de la Base de Conocimiento. Las acciones correctivas se producen cuando se detectan desviaciones y el informe cuantitativo y cualitativo se produce a partir de los informes mencionados anteriormente e incluye información sobre los recursos disponibles y adquiridos de acuerdo con la Comunicación y el Plan de Aplicación. Por último, con base en el Plan de Procesos de Medición, se genera un informe de recomendación de mejoras.

- Análisis de tendencias tecnológicas: se llevan a cabo varios análisis para determinar la viabilidad y la adecuación de las nuevas tecnologías mediante el Plan Estratégico como una guía. Como resultado, se produce un informe de la la tecnología propuesta.

Las actividades mencionadas a continuación, se utilizan para apoyar los diferentes procesos que constituyen el área de Gestión de Recursos. Se compone de tres sub-procesos de la siguiente manera:

1 GES 3.1: Recursos Humanos y Ambientes de Trabajo. Es el encargado de suministrar los recursos humanos de acuerdo a los perfiles requeridos por las funciones desempeñadas en la organización y en la evaluación de entornos de trabajo.

2 GES 3.2: Bienes, Servicios e Infraestructura. Es el encargado de seleccionar a los proveedores de bienes, servicios e infraestructura, que deberán cumplir los requisitos de adquisición de los procesos y proyectos.

3 GES 3.3: Conocimiento Organizacional. Administra la Base de Conocimientos de la Organización, la cual almacena la información y los productos producidos por la organización.

La siguiente sección describe un caso de estudio destinado a mejorar la gestión de los recursos mediante el uso de los sub-procesos y actividades introducidos en esta

sección como una guía. El estudio de caso se limita a los primeros dos sub-procesos- GES 3.1 y 3.2. – ya que el tercero (GES 3.3) está actualmente en desarrollo.

En síntesis, después de identificar la motivación de la organización (como se presentó en la sección anterior), se procedió a la elaboración de un plan de ejecución de acuerdo a las recomendaciones de Gestión de Recursos de CompetiSoft. A partir del Plan Estratégico del Sistema Judicial para el período 2005-2010, que incluyó la compra de software para la administración, y de los pasos ilustrados en la Figura 10, comenzamos la actividad A1: Gestión de Recursos .

Para ello, la actividad incluyó la evaluación de las herramientas tecnológicas para el desarrollo de sistemas de información. Debido a la naturaleza de la fuente de información, las herramientas deben ser capaces de manejar documentos de texto de manera eficiente. Para la detección de las herramientas adecuadas, se realizaron búsquedas en Internet para recoger información sobre el estado de la práctica de las diferentes tecnologías necesarias. Se analizaron las herramientas disponibles en el mercado, teniendo en cuenta aspectos como el costo, el tiempo de aprendizaje, conocer los usos, etc. Se tomaron en cuenta para realizar el análisis las "Comunidades" (conjunto de organizaciones que comparten experiencias en una herramienta en particular) existentes. De esta manera, Organizaciones (de distintas ciudades) fueron visitadas para reunir información acerca de las experiencias, lecciones aprendidas y recomendaciones. Después de evaluar las alternativas, la propuesta Tecnologica recomienda la migración de la plataforma de software de soporte a la tecnología Lotus Notes / Domino ©[15], siendo ésta base de datos documental la que resultó finalmente elegida.

[15] www.ibm.com/software/lotus/products/notes/

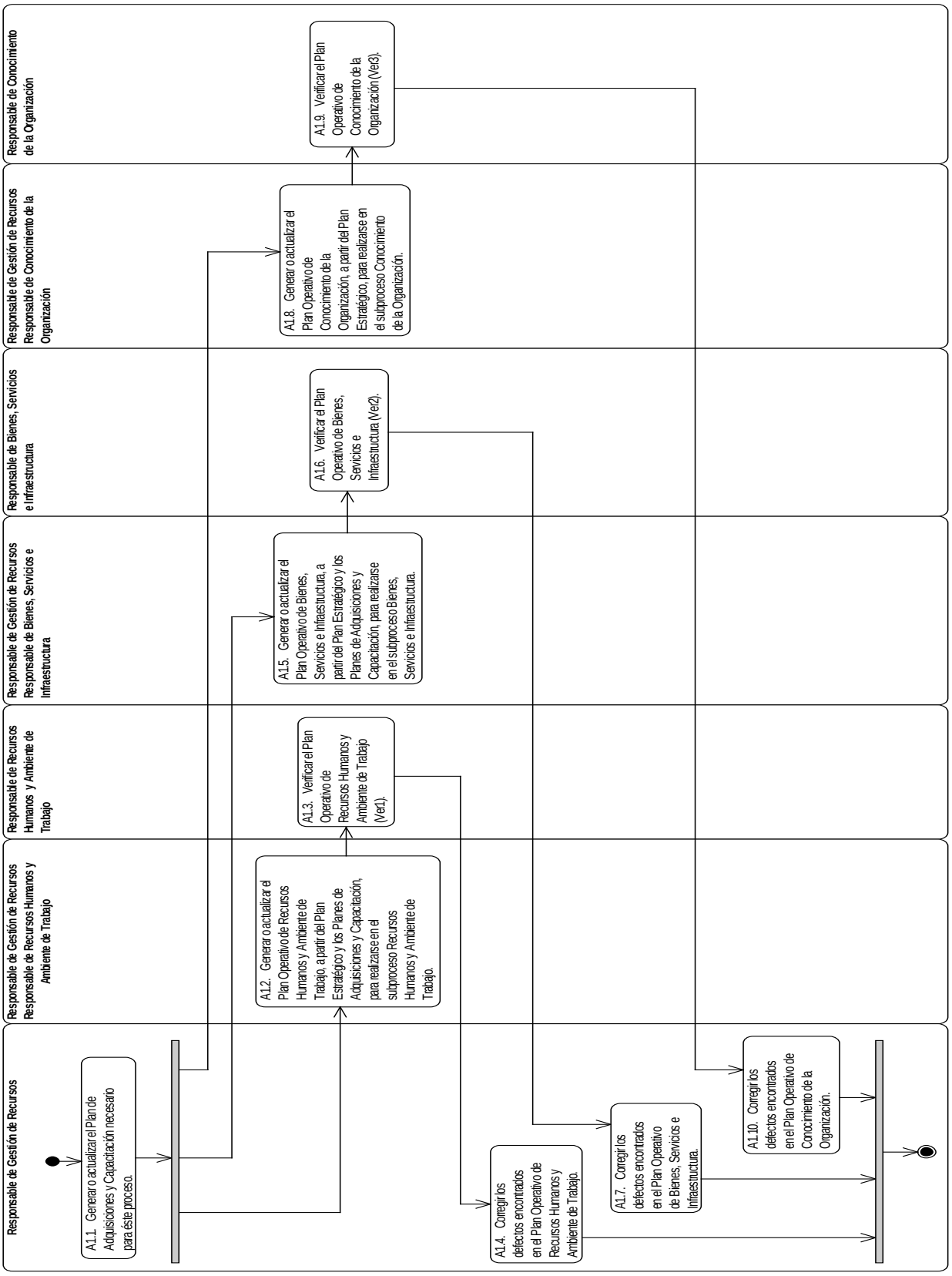


Figura 10. Diagrama de Actividades para la Gestión de Recursos

La *Actividad A1* produjo el "Plan Operativo de Recursos Humanos y Medio Ambiente", el cual fue desarrollado para la planificación de personal de la Secretaría de informática contando con la distribución de los puestos de trabajo, asignación de roles, y la evaluación de las necesidades de hardware, herramientas de software, muebles y oficinas. Del mismo modo, para elaborar el Plan de Adquisiciones y de formación, desarrollamos las especificaciones técnicas de las herramientas de software, hardware y cursos de formación. Entonces, la Administración General del Poder Judicial estuvo a cargo de la ejecución del proceso de compra de bienes y servicios, siguiendo las normas dispuestas para las adquisiciones gubernamentales (ley de administración financiera del Estado).

Tomando este plan como una entrada, empezamos a definir los equipos de trabajo reorganizando el personal, el cual estaba compuesto por tres analistas senior, dos programadores senior, dos programadores junior, y tres expertos en el dominio como consultores.

La reorganización del personal no fue una tarea fácil, teniendo en cuenta que el PJN no tenía en ejecución un proyecto de mejora de software o certificación de la calidad. La asignación de funciones a las personas - como lo requiere CompetiSoft – se realizó luego de realizar entrevistas y mediante el uso de herramientas como el MBTI (Myers-Briggs Type Indicator)[16] para identificar candidatos adecuados de acuerdo a los objetivos del Plan Estratégico.

Las funciones del proceso de gestión de recursos fueron asignadas a tres directivos del personal jerárquico de la Secretaría de Informática.

Tras el análisis de la experiencia y los antecedentes del personal, diseñamos un Plan de Formación que incluyó conocimientos básicos sobre el modelo CompetiSoft,
El plan consistió en un curso de 20 horas de CompetiSoft, 3 cursos de Lotus Notes (60 horas) que incluyó varios estudios de casos para el

[16] http://es.wikipedia.org/wiki/Indicador_Myers-Briggs

análisis, y conferencias sobre el sistema judicial, que consistió en reuniones de dos horas, dos veces por semana durante 3 meses.

Como parte de la actividad de Seguimiento y Supervisión se redefinió la información que se almacena para incluir determinados conocimientos y experiencia, y se consideró para evaluar al personal y elaborar las medidas y recomendaciones de mejora. Para producir el informe de Recursos Humanos disponibles, se utilizó la información registrada en los legajos del personal, la información sobre las posiciones anteriores, los estudios (pre-universitarios, universitarios y de postgrado), la formación, las habilidades de grupos de trabajo, y las evaluaciones anteriores.

El informe para la formación y entorno de trabajo fue construido sobre la base de cuestionarios de opción múltiple (ver Anexo I) que incluyeron:

- Relaciones interpersonales y trabajo en equipo para diseñar grupos de trabajo. Distribución de programación basada en las diferentes preferencias (tiempo completo o tiempo parcial, horarios flexibles).
- La tecnología disponible y las herramientas para apoyar el trabajo diario. Este tema nos permitió identificar las necesidades mínimas para cada estación de trabajo, como por ejemplo, conexión a Internet para acceder a bases de conocimiento, E-mail, control de versiones del sistema operativo, etc.
- Los muebles y el entorno de trabajo se rediseñaron para adaptarse al trabajo en equipo. Las personas se agruparon en cuatro grupos de personas para facilitar los debates, en tal sentido una sala de reuniones se puso a disposición para mejorar la comunicación oral. Se utilizó una pizarra blanca como un espacio común para la comunicación de noticias y avances.

Por último, respecto a las medidas y recomendaciones de mejora, hay que señalar que el tiempo de medición mostró la importancia de mantener los procedimientos de adquisición bajo control. Desde nuestra experiencia, el tiempo para la adquisición de la tecnología superó ampliamente las estimaciones, lo que dificultó la programación general provocando un impacto negativo en la motivación.

3.1.1.2 Análisis de Resultados

El uso del modelo CompetiSoft ha contribuido sustancialmente al éxito de la gestión de recursos descripta en esta investigación. Inicialmente se estableció la necesidad de entender claramente la iniciativa y luego se determinaron los objetivos y metas poniéndolas en el contexto de los objetivos y estrategias organizacionales. A partir de allí se procedió a diagnosticar el estado de situación del proceso existente y a facilitar el desarrollo de las recomendaciones y mejoras. Una de las consecuencias mas importantes de nuestra primer experiencia fue el impacto que ésta generó en las prácticas organizacionales que trascendían a la Secretaría de Informática, lo cual requirió de un trabajo interdisciplinario para adecuar las mismas.

El aprender de nuestra experiencia ha sido una excelente oportunidad para evaluar lo realizado e identificar las lecciones aprendidas, y al mismo tiempo encontrarnos con beneficios y dificultades como los que se detallan a continuación:

Beneficios

- *Staffing y entorno de trabajo*. Desarrollar estos dos planes en forma conjunta ha sido una experiencia muy positiva. Ha hecho mas fácil poder detectar aquellas cuestiones que afectaban a la motivación y a la mejorara del entorno de trabajo. La mayoría de los participantes coincidieron en que las condicione de trabajo habían mejorado.
- *Registro de productos*. La información requerida por el modelo CompetiSoft resultó conveniente desde el pto de vista cuantitativo y cualitativo para analizar el proceso. Los participantes coincidimos en que esta información contribuyó sustancialmente a comprender cómo la organización desarrolla software y adquiere los recursos necesarios para lograrlo.

Dificultades

- *Asignación de Roles.* Considerando que el programa de mejora de la calidad sólo alcanzaba a la Secretaría de Informática, se presentaron inconvenientes a la hora de establecer roles en la relación con otras áreas de la organización, lo que motivo que el área informática debiera asumir roles de gestión pertenecientes a otros sectores.
- *Selección de proveedores de bienes y servicios*. Tratandose de una organización gubernamental se debieron respetar normas muy rígidas para la contratación, que no permiten seleccionar al mejor proveedor, desde el punto de vista del cumplimiento en tiempo y forma.
- *Implementación del sistema de calidad*. Todas las actividades del modelo CompetiSoft requieren información de entrada o producen información de salida. Uno de los problemas que rápidamente advertimos fue la falta de una herramienta de software que soporte estos procesos y almacene dicha información. Lo que obligó a realizar varias tareas manuales para manejar esta informacion

Lecciones Aprendidas

- *Consecuencias de no ser prescriptivo*. Dado que CompetiSoft es un modelo de referencia, resulta dificultoso seguir las recomendaciones y aplicarlas en instituciones gubernamentales. La ausencia de los "cómo" hacer determinadas actividades y la inexistencia de frameworks de modelado exigió mayor esfuerzo a los expertos en la implementación de los programas de mejora de la calidad. Esta situación es común a todos los modelos de calidad.
- *Disponibilidad de los recursos humanos*. Dado que la SI es un área orientada a servicios, ésta requiere una gestión enfocada al uso racional de los recursos de acuerdo a las tareas planificadas y a las solicitudes de usuarios. Esto conlleva a un debate entre lo urgente y lo importante, el cual exige una gestión permanente en la asignación de recursos.

- *Adquisición de recursos tecnológicos*. Las entidades gubernamentales padecen una excesiva burocracia en el proceso de compra de bienes y servicios, producto de los numerosos controles para evitar irregularidades. Esto le agrega demoras que a veces entran en conflicto con la disponibilidad con la que cuentan los proveedores. Para mitigar esta situación se creo un nuevo rol llamado "supervisor del proceso de adquisición" que es quien se encarga del seguimiento del proceso de compra, para solucionar los problemas derivados de requisitos administrativos.
- *Mediciones*. Es importante saber que un modelo de calidad va incorporando actividades que en principio no están bien definidas y se van depurando en la práctica, esto hace necesario ir tomando mediciones de estas actividades, donde se reflejen los desvíos para corregir las estimaciones realizadas durante la planificación. Por lo que resulta imperioso contar con una base de conocimiento para utilizar y retroalimentar en los sucesivos proyectos.

3.1.2. Definición y Fortalecimiento de la Estructura para Soporte a Usuarios

Además de trabajar en la aplicación de distintos aspectos de estándares de calidad como la gestión de recursos expuesta precedentemente, se inició una mejora en el proceso de desarrollo de software. Como mencionábamos anteriormente el e-gov representa un servicio que el estado debe darle a los ciudadanos con el objeto de optimizar los recursos para su funcionamiento. En tal sentido el hecho de utilizar herramientas tecnológicas para atender a los ciudadanos, sólo se convertirá en una relación beneficiosa para ambas partes si ésta funciona adecuadamente en tiempo y forma, es por ello que los sistemas que se utilicen para brindar el mencionado servicio deben ser efectivos y eficientes. Siguiendo éste lineamiento, la Secretaría de Informática ha emprendido una mejora del proceso de software (SPI).

Como primer paso se identificaron las fortalezas y debilidades del proceso de software utilizado por la organización para determinar las acciones efectivas de la mejora.

3.1.2.1 Iniciativa de Mejora

Nuestra iniciativa de SPI se enfocó en la mejora de la satisfacción del usuario para proyectos de desarrollo de software específico. En primer lugar vamos a definir lo que significa para nosotros el concepto de "satisfacción de usuario" en nuestro contexto: la Secretaría de Informática recibe requerimientos para desarrollo de nuevas aplicaciones y para mantenimiento de las existentes, esto implica considerar procesos en dos niveles diferentes: Nivel Operaciones, que incluye procesos de desarrollo y mantenimiento; y Nivel de Gestión Media, que incluye practicas de gestión de proyectos.

La iniciativa de SPI involucró a 20 personas de la organización, y 1 consultor de la Academia durante 8 meses, lo que resultó en 1600 horas hombre.

Se utilizó el modelo de mejora PM-Competisoft a partir del cual planificamos cada valoración definiendo su propósito, alcance, recursos y responsabilidades, e infraestructura.

Dividimos la planificación en una fase inicial y una fase de refinamiento; de esta manera iniciamos el ciclo y fuimos diagnosticando el proceso. Para ello definimos indicadores de proceso y recolectamos datos con entrevistas a distintas agencias gubernamentales con diferentes puntos de vista (gerentes, desarrolladores, consultores de tecnología, programadores, etc) de los departamentos de sistemas.

Asi mismo se analizaron artefactos, como planes de proyectos y documentación de productos de software, para luego analizar los datos a través de la correspondencia con el modelo de evaluación. En general se llevo adelante la evaluación por periodos de 3 días (no necesariamente consecutivos), sin incluir el tiempo ocupado en preparar el reporte de evaluación. Basados en nuestros interrogantes de investigación, nuestra contribución se basó en diferentes aspectos de la satisfacción del usuario. Como resultado obtuvimos una primera lista de fortalezas y debilidades que los representantes de entes gubernamentales sólo conocían en forma parcial.

En principio direccionamos el proyecto de gestión de procesos utilizando el modelo Competisoft, con su grupo de gestión de procesos. Evaluamos cinco grupos de procesos (Inicio, Planificación, Ejecución, Monitoreo y Cierre) utilizando el cuestionario de evaluación que fuera validado por los distintos sectores de sistemas entrevistados. El resultado mostró que sólo los tres primeros grupos de procesos estaban en el nivel 1 (Realizado) del modelo PM-Competisoft (ver Tabla 2), mientras que los otros dos grupos quedaban incompletos.

Tabla 2. Niveles de Madurez de CompetiSoft

Nivel	Capacidad del Proceso
0	Incompleto
1	Realizado
2	Gestionado
3	Establecido
4	Predecible
5	Optimizado

En segundo lugar nos enfocamos en las fases del desarrollo de software utilizando el modelo de referencia Competisoft, y evaluamos utilizando los cuestionarios. Como resultado encontramos que todas las fases (Inicio, Requerimientos, Análisis, Diseño, Codificación, Integración, Verificación y Cierre) estaban en el nivel 1 (Realizado).

Enfocándonos en la satisfacción del usuario, encontramos tres niveles destacables para soportar los procesos. En el nivel 1 identificamos el Front-Desk donde los representantes de sistemas reciben las inquietudes, donde cada inquietud es analizada y requiere dar una respuesta. Sin embargo hay inquietudes que requieren un mayor análisis antes de poder encontrar una solución y éstas forman parte del Nivel 2. De manera similar, existen inquietudes del Nivel 2 que requieren un análisis todavía mayor, a éstas las consideramos como de Nivel 3, en éste caso el análisis es complejo y muy probablemente requiera de la intervención de expertos y uso de bases de conocimiento.

Los indicadores que incluimos, expresados como promedios, son los siguientes:

- Media de tiempo de respuesta para resolver un problema (MTRP)
- Numero de tareas realizadas por problema resuelto (NTRPR)
- Requerimientos promovidos por semana Nivel 1 a 2 (RPS1) y Nivel 2 a 3 (RPS2)

Antes de recolectar y analizar la información, se calcularon los indicadores para ver cual era el estado de situación actual. De 150 requerimientos catalogados como de nivel 1 calculamos los siguientes valores:

- MTPR - Media de tiempo de respuesta para resolver un problema: 96
- NTRPR - Número de tareas realizadas por problema resuelto: 5
- RPS1 - Requerimientos promovidos por semana Nivel 1 a 2: 120
- RPS2 - Requerimientos promovidos por semana Nivel 2 a 3: 80

Los indicadores muestran que de 150 requerimientos, el 80% fueron catalogados como de Nivel 2 y de ellos el 66% se consideraron en el Nivel 3. Esta diferencia nos muestra que para resolver un problema se requiere tiempo extra para analizar, lo que afecta el tiempo de respuesta. En el caso de estudio se estableció un promedio de 96 hs.para atender un requerimiento.

Los representantes de los departamentos de Sistemas reconocieron esta situación y trabajaron para identificar las causas de la insatisfacción. Así mismo se identificó que no existía un repositorio de documentación para hacer un seguimiento y facilitar el proceso de análisis y solución y no existía un procedimiento formalizado de documentación para poder hacer una revisión. Por lo tanto, no existía visibilidad de etapas y procesos, y no había una base de datos de conocimiento para poder buscar soluciones existentes (ya aplicadas) a problemas nuevos. Con esta evidencia se planteó un programa de mejora basado en atender estas falencias.

Se formuló una propuesta de mejora que balanceara la documentación con la experiencia, para que la burocracia de registrar información no se convirtiera en un condicionante que atentara contra la mejora, y que a la vez no faltara información documentada a la hora de analizar el problema y gestionar la solución. El principal objetivo era entonces extraer y documentar la información relevante para analizar el problema.

Sugerimos comenzar con una experiencia piloto, que incluyera descripción de procesos, buenas prácticas, plantillas, y datos en un repositorio de conocimiento simple. Además incorporamos relaciones simples entre estos elementos. También sugerimos almacenar los documentos en un repositorio separado; del mismo modo se definieron roles y responsabilidades para manejar cada uno de los elementos mencionados.

Finalmente, las mejoras se fueron incorporando de manera incremental (ver Figura 11), separando la gestión del desarrollo. Como puede verse, elaboramos un plan de mejora, que involucraba la definición de un work-flow de tareas, para poder hacer las tareas, actividades y procedimientos más visibles.

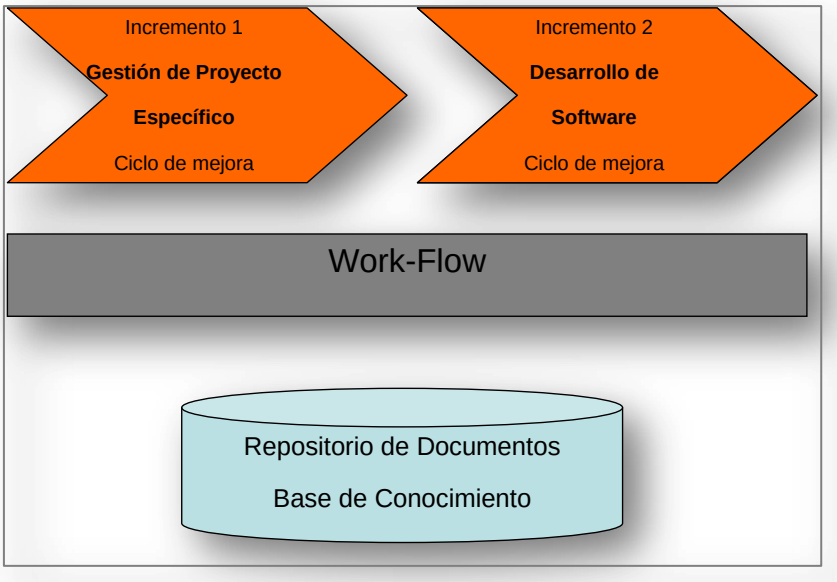


Figura 11. Incorporación de Mejoras en Modalidad Incremental

3.1.2.2 Análisis de Resultados

De las primeras mediciones a través de cuestionarios con el usuario, se reveló un incremento considerable en la satisfacción del cliente (60%), y esto es gracias a que la calidad del servicio fue mejor comprendida.

El hecho de haber incrementado la visibilidad del proceso de atención al usuario, le ha permitido a la SI reducir el tiempo para clasificar el problema y encontrar las soluciones potenciales. Luego de implementar las mejoras resultó muy alentador encontrar un MTRP de 48, lo que significó una mejora del 50%, es decir que se redujo a la mitad el tiempo para dar respuesta a un problema.

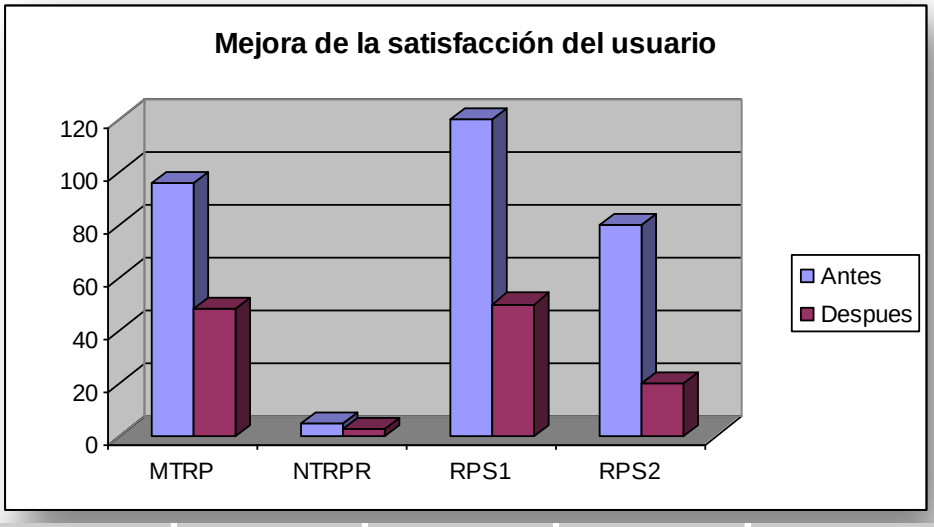
El NTRPR también se redujo, a causa de una mejor asignación de roles, actividades y una mejor compresión de los problemas planteados. El valor encontrado para el NTRPR fue de 3 (60% de reducción). El factor que más influyó para esta reducción fue el uso de repositorios de información (documentos y conocimiento) para soportar la identificación y clasificación de los problemas. A pesar de la simplicidad de los datos almacenados, el hecho de contar con repositorios estructurados, le permitió al personal pensar en soluciones de una manera más eficiente que apelar sólo a su memoria, lo que contribuyó a reducir los recursos humanos utilizados.

Finalmente, las mediciones de los RPS, de acuerdo a los 3 tipos de niveles definidos, también resultaron promisorias. La cantidad de asistencias en el nivel 1 ascendió a 200, mostrando que durante la experiencia se dieron más requerimientos de diferentes organismos. Sin embargo, solo 50 de ellos (25%) requirieron un análisis mayor y en consecuencia fueron promovidos al nivel 2, y de ellos solo 20 requirieron un análisis mas complejo (40%), por lo que se los clasificó como de nivel 3.

En el gráfico de la Figura 12 podemos observar un incremento del 33% en los requerimientos, donde la SI fue capaz de filtrar los requerimientos básicos de los complejos; es decir que se logró clasificar los requerimientos basados en necesidades

reales de un mayor análisis, lo que dio lugar a un uso mas eficiente de los recursos humanos. Los requerimientos de nivel 2 y 3 fueron realmente específicos (reducción del 58% y 75%) respectivamente.

La iniciativa de SPI intenta cambiar el "cómo" la gente lleva adelante el diseño del proceso de software, en tal sentido, el SPI es una herramienta para la mejora del diseño a nivel organizacional, particularmente en las organizaciones gubernamentales. Asumimos esto como verdadero, y basado en como realizamos las mejores prácticas dentro de la SI, intentamos generalizar el uso como un modelo formal de SPI.



	MTPR	NTRPR	RPS1	RPS2
Antes	96	5	120	80
Después	48	3	50	20

Figura 12. Indicadores de la Mejora de la Satisfaccion de Usuarios

Los resultados preliminares son promisorios, sin embargo éstos están limitados a nuestro caso de estudio. Actualmente el número de tareas (NTRPR) cuenta actividades sin tener en cuenta la complejidad o granularidad, esto implica que las tareas complejas o las simples son consideradas por igual. Esta situación pude generar una subestimación, pero no invalida la mejora implementada, ni sus buenos resultados. Así

mismo entendemos que la reasignación de recursos no es un proceso trivial, pero hacer que esos recursos hayan quedado disponibles es un beneficio en si mismo.

De la misma manera no se ha incorporado un análisis de complejidad o granularidad respecto a los requerimientos recibidos (MTPR) en el front-desk, lo que podría llevar a una interpretación errónea cuando decimos que se redujo de 96 a 48 hs. Creemos que encontrar una solución para un problema complejo demanda más esfuerzo y tiempo que para un problema simple. Esta situación fue tenida en cuenta al momento de seleccionar las muestras de requerimientos, en tal sentido hemos controlado la diversidad de requerimientos antes y después de aplicar la mejora.

De la experiencia podemos enunciar las siguientes lecciones aprendidas:

- *Necesidad de compromiso y supervisión*: Dado que la SI es un área orientada a servicio, requiere de una asignación racional de los recursos a las diferentes tareas planificadas, contemplando los imprevistos que puedan surgir como urgencias, lo cual involucra una constante revisión de prioridades, dando lugar al debate entre lo urgente y lo importante. Es por ello que se requiere un compromiso y supervisión constante para lograr un balance acertado entre lo planificado y lo imprevisto.
- *Visibilidad de productos y procesos*: Nuestra experiencia mostró mayor visibilidad de productos y procesos (estructurando y registrando documentación y conocimiento) que impactó fuertemente en la asistencia a usuarios. Fuimos desde un proceso de características "caóticas" a un proceso estandarizado y comprensible, capaz de resolver los requerimientos de usuario en menos tiempo y con mayor precisión y efectividad. Por supuesto que es fundamental contar con una herramienta de software que soporte dicho proceso para llegar a buenos resultados.
- *Consecuencias de no ser prescriptivo*: Dado que Competisoft es un modelo de referencia, seguir sus recomendaciones y aplicarlas en una organización gubernamental es más dificultoso que hacerlo en una empresa privada, esta

situación demandó un mayor esfuerzo de los especialistas en calidad para respetar las recomendaciones del estándar, definiendo los "cómo" hacer cada tarea. De todos modos esta es una situación que se da comúnmente en la aplicación de muchos de los modelos de mejora.

Haber trabajado en la construcción de éstos dos pilares permitió sentar las bases para luego comenzar a pensar en prácticas de gobierno electrónico como expondremos en el Capítulo 4. Poder contar con un proceso previsible y rastreable para la gestión de recursos que requieren los proyectos de software resulta indispensable en una organización gubernamental, ya que su ausencia atenta contra la concreción de los proyectos que luego se transformaran en servicios de e-gov. Así mismo la visibilidad de productos y procesos inherentes a la respuesta de inquietudes de usuario para el desarrollo de nuevo software o mantenimiento del existente, es condición necesaria para que los servicios de e-gov puedan ser sustentables y mantenibles en el tiempo, máxime si se piensa en reemplazar, dentro de un futuro no muy lejano, a los procesos manuales y de atención personalizada que se llevan adelante hoy en día.

4 GUÍAS Y LECCIONES EN LA INTRODUCCIÓN DE PRÁCTICAS: FIRMA Y NOTIFICACIÓN ELECTRÓNICA

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel. Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. El uso de dicha herramienta no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente. La firma digital es un instrumento con características técnicas y normativas, ésto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen[17].

La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados. El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir. Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo[18].

[17] http://www.jgm.gov.ar/paginas.dhtml?pagina=264

[18] http://www.jgm.gov.ar/paginas.dhtml?pagina=262

En la elaboración de una firma digital y en su correspondiente verificación se utilizan complejos procedimientos matemáticos basados en criptografía asimétrica (también llamada criptografía de clave pública). En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica de que si bien están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda, ni tampoco a partir de los documentos cifrados con la clave privada. El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma. En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona. En algunos casos, puede ser necesario crear una cadena de certificados, cada uno certificando el previo, para que las partes involucradas confíen en la identidad en cuestión. En su forma más simple, el certificado contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo. Su formato está definido por el estándar internacional ITU-T X.509[19]. De esta forma, puede ser leído o escrito por cualquier aplicación que cumpla con el mencionado estándar. En la Figura 13 vemos como funciona el esquema de firma digital.

[19] http://www.jgm.gov.ar/paginas.dhtml?pagina=262.

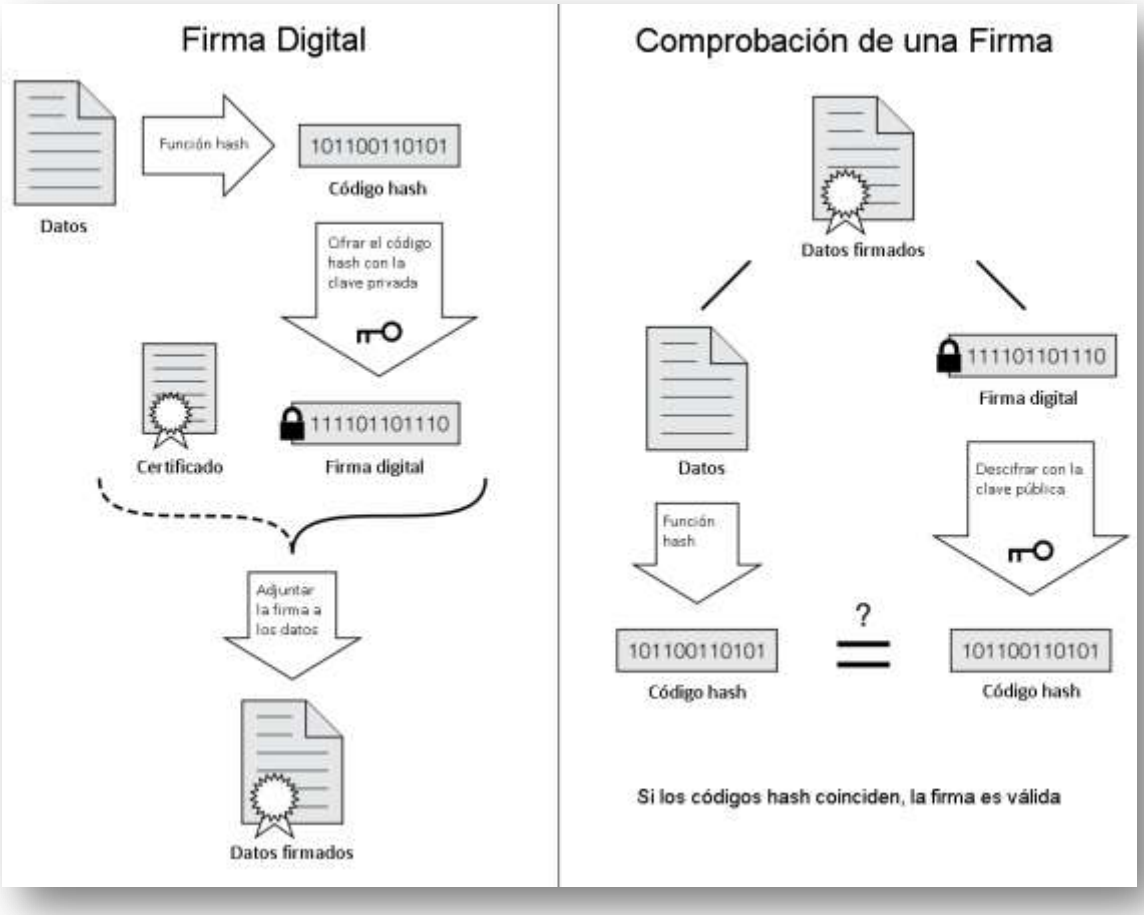


Figura 13. Funcionamiento de la Firma Digital

4.1 Firma Digital en la Legislación Argentina

Para la legislación argentina los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la "Firma Digital" existe una presunción "iuris tantum" en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, de ser desconocida por su titular, corresponde a quien la invoca acreditar su validez. Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un certificador licenciado (o sea que cuente con la aprobación del Ente Licenciante). La

legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" utilizado por la Comunidad Europea[20] o "Firma Electrónica" utilizado en otros países como Perú, Chile o Costa Rica[21].

En nuestro país se denomina "Infraestructura de Firma Digital" al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes (por ej. Internet)[22]. Realmente esta definición es conocida mundialmente con las siglas PKI que significan Public Key Infraestructure o Infraestructura de Clave Pública.

4.1.1. Notificación Electrónica

Tomando como base el estudio realizado por el Dr. Héctor Mario Chayer[23], Director Académico del Foro de Estudios sobre la Administración de Justicia, respecto a las alternativas de implementación de la notificación electrónica en los procesos judiciales, podemos argumentar que la sociedad se ha visto transformada con la aparición de las nuevas tecnologías de la información y las comunicaciones (TICs). La disponibilidad de una red como Internet es un indicador importante del impacto que tienen hoy. Para las telecomunicaciones, el tráfico comercial y el entretenimiento, por mencionar sólo tres áreas, estas tecnologías son prácticamente indispensables. En ellas, al igual que en muchas otras, es imposible alcanzar resultados económicos aceptables y beneficiosos, tanto para los particulares como para la sociedad en general, sin su utilización. Esto es perfectamente aplicable al sistema judicial, que para cumplir con su función de

[20] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica. http://www.cert.fnmt.es/legsoporte/directiva.PDF

[21] Ley de Firmas de Perú. http://www.congreso.gob.pe/ntley/Imagenes/Leyes/27269.pdf

Sistema de Certificación de Costa Rica. http://www.firmadigital.go.cr/index.html

Ley de Firmas Chile - Ley 19799: http://repositorio.idiem.cl/ley19799.pdf

[22] Ley argentina de firma digital 25.506: http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[23] Publicado en Derecho Informático 3, Editorial Juris, Rosario, Argentina Noviembre de 2002

administrar justicia básicamente debe tratar información en cantidades crecientes. Sin embargo, mientras se mantenga el paradigma del soporte papel en los expedientes judiciales, resulta inexacto hablar del expediente digital. Pues aunque se utilicen sistemas de gestión con procesadores de textos, si finalmente las providencias o las peticiones de las partes deben imprimirse en papel y firmarse, para luego coserse al expediente, y ser eventualmente copiadas a mano, para retipearse en escritos que las citen, y trasladadas físicamente hasta las partes para notificarlas, las potencialidades de las tecnologías de la información se reducen a una mínima expresión. Pero en relación al impacto en el sistema judicial de las tecnologías de la información, abordaremos solo un tema, el uso de las potencialidades comunicacionales de las TICs para las notificaciones judiciales, por tratarse de una cuestión con un debate abierto, grandes potencialidades transformadoras y escasas concreciones.

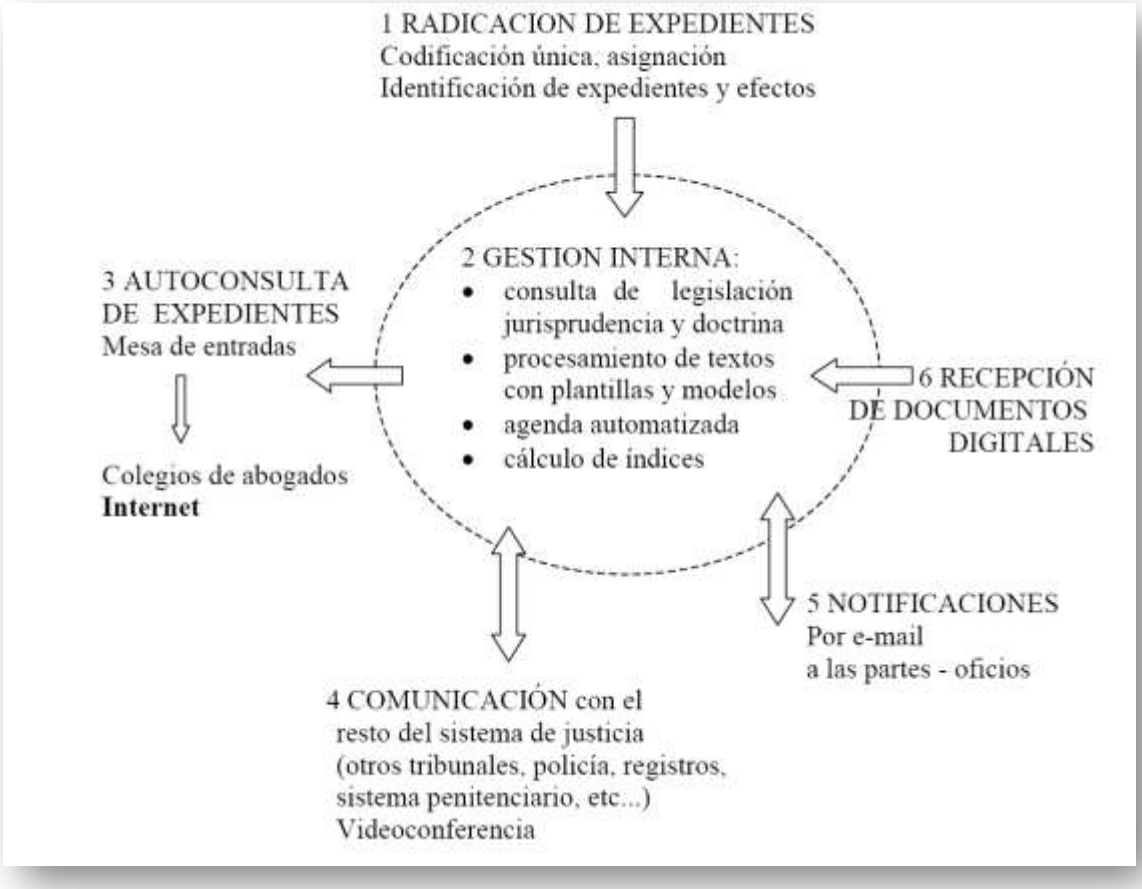


Figura 14. Esquema de Trabajo para Notificaciones Electrónicas

En la Figura 14 se ilustra el esquema de trabajo, en donde se enuncian las principales tareas propias de la gestión judicial que pueden ser realizadas de modo más rápido y a menor costo con el uso de las nuevas tecnologías. Puede apreciarse entre ellas el uso de las facilidades comunicacionales para las notificaciones, como el último hito previo a la recepción de documentos en formato digital. Cuando todos estos procesos estén implementados, el expediente totalmente digital será una realidad.

4.1.1.1. Las Notificaciones Procesales

Las TIC´s están llamadas a revolucionar no sólo el procesamiento, almacenamiento y recuperación de los escritos que componen un expediente judicial para transformarlo en íntegramente digital, sino también el modo en que los tribunales, los terceros y las partes se comunican, incluyendo esto último la comunicación judicial por excelencia, que es la notificación procesal.

Abordemos entonces el análisis de las notificaciones en tanto actos procesales de comunicación. Etimológicamente, notificación proviene de la voz latina notificatio, compuesta por nosco, -ere ("conocer") y facio, -ere ("hacer"); es decir, significa "hacer conocer". Atañen al derecho de defensa en juicio consagrado en el art. 18 de la Constitución Nacional, de lo que deriva su importancia indiscutible, ya que el principio de contradicción exige que las decisiones judiciales no se adopten sin previo traslado a la parte contra la cual se han solicitado, a fin de darle una oportunidad de defensa.

La doctrina ha debatido si debe primar el principio de la recepción o el del conocimiento. La primer teoría sostiene que las notificaciones producen plenamente sus efectos cuando han sido observadas las normas legales para que el acto notificado llegue a su destinatario, con prescindencia del conocimiento efectivo que se tenga de su contenido. La teoría del conocimiento considera que la falta de notificación o su deficiencia no es condición suficiente para negar eficacia notificatoria al conocimiento del acto obtenido por otros medios. "El principio del conocimiento funciona supletoriamente (ante la falta o irregularidad del acto de notificación), siempre que de

las circunstancias del caso concreto se pueda inferir lo inequívoco de él"[24]. Este planteo es de la mayor importancia para sustentar la factibilidad de las notificaciones electrónicas aun con el marco jurídico actual. Pues es obvio que ante esta actividad comunicacional de los procesos judiciales, de una envergadura superior a los 12 millones de cédulas anuales sólo en la provincia de Buenos Aires[25], las TICs ofrecen varias alternativas, distintas entre sí por las herramientas técnicas, los efectos jurídico-procesales y de reconfiguración de los métodos de trabajo actuales; ninguna de las cuales tiene consagración legislativa. Sin embargo, en la actualidad, aun sin un marco normativo, consideramos que el uso de herramientas electrónicas para la notificación, tal como la han practicado por cualquier medio el Dr. Labrada en Pergamino, o con el correo electrónico, entre otros, el Juez Toribio Sosa en Trenque Lauquen y la Cámara Laboral de Bariloche, están protegidas por el principio de saneamiento, admitiendo que la notificación surte efectos cuando "del expediente resultare que la parte ha tenido conocimiento de la resolución"[26], aunque no se haya seguido un camino ortodoxo para notificarla. Podemos hablar de una notificación tácita, de interpretación restrictiva, donde es inoperante plantear la nulidad por la nulidad misma, por lo que no se podría cuestionar el medio utilizado cuando, a través de él, se hubiere obtenido claro anoticiamiento[27].

La jurisprudencia ha recogido estos conceptos en la práctica, aplicándolos a distintos supuestos[28]; cabe agregar, además, que quien impugna de nulidad un acto, de

[24] Alberto L. Maurino, *Notificaciones procesales,* pág. 9, 2da edición, Editorial Astrea, Buenos Aires 2.000.

25 En el fuero penal hay 3.000.000 que van por vía judicial y 3.700.000 que efectúa la policía; los demás fueros totalizan otras 5.300.000.

[26] Art. 149 del Cód. Proc. Civil y Com. de la Prov. de Bs. As.; en el mismo sentido, el art. 149 del Cód. Proc. Civil y Com. de la Nación y el art. 69 del Cód. Proc. Civil y Com. de Santa Fe.

[27] Esto es en virtud de la aplicación del art. 172 Cód. Proc. Civil y Com. de la Prov. de Bs. As.

[28] Por ejemplo, quien se queja de la irregularidad que consiste en la falta de certificación del envío de una cédula por correo, no puede hacerlo sin negar su recepción (CCivCom Rosario, Sala II, 8/10/70, Juris, 38-110); o en el caso de un ente social, no puede argüirse que la diligencia notificatoria no ha logrado su finalidad específica cuando se ha dirigido al presidente de la accionada, siendo que el natural

notificación, debe expresar fundadamente y acreditar la existencia de un perjuicio. Compartimos con Toribio Sosa[29] que son claramente distinguibles dos partes en los códigos procesales: primero, la conformada por todos los preceptos que establecen cómo deben ser efectuados los actos procesales; y segundo, el capítulo (o mejor, el régimen) de las nulidades procesales, de cuyo articulado es posible extraer bajo qué resguardos los actos que no se hagan en la forma prevista por el otro grupo de normas (mayoritario, ciertamente) resultan igualmente válidos. Dicho de otra manera, una cosa son las normas que dicen cómo hay que hacer los actos procesales, y otra cosa son las normas que dicen que, en caso de no hacerse así, igual pueden valer. En conclusión, los actos procesales *válidos* pueden ejecutarse de dos modos:

a. de forma regular, esto es, como lo establecen las normas procesales que los regulan;
b. de forma irregular o alternativa, es decir, no como lo prevén las normas procesales que los regulan, pero sin llegarse a reunir los recaudos indispensables como para provocar su invalidación.

Es aquí donde hacemos pie para sostener la viabilidad del uso de la notificación por medios distintos a los tradicionales, con riesgos calculados, previa inmunización contra la nulidad procesal. Se trata de realizar sistemáticamente actos procesales que, aunque no se ajusten estrictamente a las pautas procesales que específicamene los regulan, igualmente no puedan ser declarados nulos.

El planteo podría formularse así: *si un acto procesal irregular o alternativo (en el caso que nos ocupa, la notificación por medios técnicos sin el soporte papel)) cumple la finalidad que está llamado a llenar (art. 169 3er. párrafo CPCC), si la distinta*

conocimiento del acto de citación no se ve afectado po el hecho de que se la haya dirigido a su domicilio real (CNCom, Sala A, 15/4/75, ED, 63-254).

[29] Para este análisis resulta sumamente esclarecedor el artículo "La reingeniería procesal" del Dr. Toribio Enrique Sosa (publicado en línea en www.lex-doctor.com/publica/varios/ sosa1.htm) sus ideas se siguen, a la letra en muchos casos, en las líneas desarrolladas a continuación.

modalidad es provocada o consentida expresa o tácitamente por las partes (arts. 170 2do. párrafo y 171 CPCC), si no causa perjuicio alguno a las partes (art. 172 1ra. parte CPCC), y si además promueve una mayor eficiencia del servicio de justicia, no hay obstáculo para realizarlo así.

Es evidente que no está reglamentado su uso por las normas procesales; pero si las partes consintieran expresamente su utilización no podría objetarse su uso; para lo cual resulta conveniente una resolución que la dispone (mejor, si con el consenso previo y expreso de las partes, en cuyo caso cabría hablar de correo electrónico "constituido", con el compromiso de consultar a diario dicha casilla de correo). Así, desde el año 1996 en el Juzgado Civil y Comercial No 1 de Pergamino, en la providencia simple que ordena el traslado de la demanda, el Dr. Labrada incorpora una frase que dice: "luego de notificada la demanda, las providencias en que se ordene notificar personalmente o por cédula a las partes y/o sus letrados, se considerarán cumplidas al ser realizadas por cualquier medio que produzca un resultado fehaciente, excepto la sentencia"[30]. Al quedar consentida, se convierte en una regla procesal que deberán respetar las partes, pudiendo los abogados elegir los medios que consideren mas convenientes (sea carta documento, nota con acuse de recibo, fax, etc…) procurando preconstituir la prueba para el caso que fuera negada la recepción de la notificación o su contenido.

Se trata entonces de llevar a cabo actos procesales de notificación alternativos o irregulares, pero válidos, por adoptarse los recaudos necesarios como para que la irregularidad no pueda trocarse en nulidad procesal.

En definitiva, podemos decir que al distinguirse el marco que regula los actos de notificación, del sistema general que regula las nulidades en el proceso, las notificaciones por correo electrónico exitosas hoy constituyen un acto procesal irregular (en tanto no regulado) pero válido (en tanto cumplió sus fines)[31]. Dicho todo lo cual, no

[30] Pelayo Ariel Labrada, Diez claves para la celeridad procesal sin reformas legislativas, pág. 5, edición de autor, 2.000.

[31] Un detallado análisis de los presupuestos de nulidad de las notificaciones, con abundante casuística, puede encontrarse en Alberto L. Maurino, op. cit., pág. 353 a 370.

debe olvidarse que el derecho de defensa en juicio de las partes, derecho del cual las normas de los códigos procesales constituyen reglamentación, no debe en ningún caso ser sacrificado en aras de la eficiencia del servicio.

4.1.1.2. Nociones Jurídicas Básicas

Antes de abordar las alternativas posibles para instalar definitivamente los medios tecnológicos hoy disponibles en el campo de las notificaciones procesales, cabe repasar una serie de nociones jurídicas básicas relativas a las notificaciones y los domicilios, que serán de suma utilidad para encuadrar la discusión.

En primer lugar, recordemos que existen cuatros tipos básicos de notificación regulares (por oposición a las irregulares, alternativas o no reguladas que arriba mencionábamos y que luego retomaremos). Así, tenemos que la notificación por excelencia es la *notificación personal* o en el expediente, en la que el interesado conoce realmente la resolución transmitida (sea voluntaria, cuando el interesado libremente deja constancia de la forma indicada por las normas procesales, o coactiva, cuando estando obligado a notificarse, se negare a hacerlo y valga como tal la atestación que acerca de su negativa realice el funcionario autorizado[32]; dicho esto sin perjuicio de que en la práctica este último régimen no se cumple). Este tipo de notificación suple a cualquiera de las otras especies.

En segundo lugar, la notificación automática o *ministerio legis* es la regla, ya que las partes están a derecho con la primera notificación recibida. Si bien es un tipo de notificación ficta, puesto que no existe un acto real de transmisión sino un conocimiento presunto por ficción de la ley, coincidimos con Eisner cuando considera que "… cumple

[32] V.gr. art. 142 Cód. Proc. Civil y Com. de la Prov. de Bs. As, art. 142 Cód. Proc. Civil y Com. de la Nación, art. 60 Cód. Proc. Civil y Com. de Santa Fe.

su función, permite el avance del proceso en celeridad y descargado de costos, y deja en mano de los litigantes cuidar su interés y estar atento al desarrollo de la causa"[33]. Se tiene por operada determinados días de la semana preestablecidos, aunque el interesado no comparezca a la sede judicial, y por tanto ignore la resolución correspondiente. Obsta a su cumplimiento que el expediente no esté en letra o en secretaría el día fijado, y que tal circunstancia se haga constar en un libro de asistencia. Estos requisitos procuran equilibrar y armonizar la celeridad y economía procesal con la garantía de defensa en juicio.

En tercer lugar, la *notificación por cédula* es una excepción a la regla general de la notificación automática, que la doctrina nacional coincide en considerar un sistema con más defectos que virtudes[34]. Pero contrariamente a lo que debería ser, es la notificación más común de las expresas, y su tramitación es responsable de gran parte de los tiempos de duración de los procesos judiciales, ya que se hace a domicilio por medio de un oficial notificador, que entrega una cédula. Esta cédula es un instrumento público expedido por un funcionario judicial (quien debería redactarlo y diligenciarlo, no las partes), cuyo original se agrega a los autos y la copia se entrega al notificado. La diligencia de notificación (que en general se asienta al dorso de la cédula original que se devuelve al expediente) configura también un instrumento público, en los términos del art. 979 inc. 2º y 4º del Código Civil, pues emana de un funcionario público en la forma prescripta por las leyes, haciendo plena fe mientras no se ataque su validez. El contenido de la cédula se encuentra generalmente regulado en detalle, así como los supuestos en que procede este tipo de notificación[35]. Corresponde distinguir, siempre dentro de esta categoría, el traslado de la demanda y algunas otras resoluciones, que

[33] Isidoro Eisner, Notificaciones fictas, tácitas y compulsivas en el proceso civil, LL, 139-1202.

[34] En tal sentido se pronuncian Lino Palacio, Derecho Procesal Civil, t. V, pág. 360, Buenos Aires, Abeledo Perrot, 1977; Ramiro Podetti, Tratado de los actos procesales, t. II pág. 272, Buenos Aires, Ediar, 1955.

[35] Por ejemplo, el art. 135 Cód. Proc. Civil y Com. de la Prov. de Bs. As. enuncia en que casos procede, y remite también a los supuestos reglados en otras disposiciones y a la facultad del juez para ordenarla por resolución fundada en los casos no previstos.

deben hacerse al domicilio real, dentro de una interpretación restringida que procura asegurar el derecho de defensa en juicio, de la mayoría de las notificaciones por cédula, que se dirigen al domicilio procesal constituido ad hoc.

Consideramos a su vez especies dentro de esta categoría a la notificación por correo (abarcativa de la postal y telegráfica) y a la notificación en los estrados del juzgado. La primera de estas especies es un tipo de notificación mediante cédula, con la sola diferencia en la vía de transmisión o llegada al destinatario. Diversos sistemas legales de nuestro país lo autorizan (Córdoba, Santa Fe, la Nación –si bien con restricciones, Entre Ríos, Chaco y la Prov. de Buenos Aires), a solicitud de parte interesada. La fecha de la notificación es la de la constancia de la entrega al destinatario; si es inhábil, el plazo empieza a correr a las 0 horas del primer día hábil inmediato posterior. Dado su carácter recepticio, el aviso de recepción es esencial y debe agregarse al expediente (equivale a la diligencia de notificación del oficial notificador). Decíamos que incluíamos aquí a la notificación en los estrados del juzgado, pues no se trata de una notificación automática, sino un acto real de trasmisión a un domicilio constituido, elegido por la ley como sanción por no haber determinado el litigante el domicilio procesal de su gusto. Si bien cierta parte de la doctrina lo ha sugerido, no es necesario expedir la cédula respectiva cuando corresponde notificar personalmente o por cédula. De todos modos, su regulación en general es poco clara, y lleva a confundirla con la notificación automática.

Finalmente, el último tipo de notificación regulado en la legislación adjetiva nacional es la *notificación por edictos*. Esta se prevé para notificar a personas desconocidas, o conocidas cuyo domicilio se ignora, o ante la actitud reticente del destinatario, o cuando en general media una imposibilidad de recurrir a otras formas de notificación. Se puede describir como un acto de notificación expreso, ya que opera mediante un acto real, aunque generador de conocimiento presunto. El edicto tiene los mismos contenidos que la cédula, aunque resumidos; y se publica en la prensa escrita; a pedido del interesado, puede difundirse por la radio, la televisión o aun en las tablillas del juzgado (en casos de escaso monto económico). Se impone cada vez con más fuerza la conciencia de que se

trata de una ficción inútil por inoperante, de esperable desaparición en un buen régimen procesal.

La segunda noción que consideramos necesario retomar es la del *domicilio y sus distintas clases.* Su importancia deriva de ser un elemento determinante del ámbito de las notificaciones, al ser el *centro de recepción o envío de comunicaciones, que se ve impactado de lleno por las transformaciones en el concepto del espacio que las TICs han impuesto.*

El domicilio real es definido concordantemente como el asiento jurídico de la persona, siendo el lugar de su residencia efectiva. Las notificaciones iniciales del proceso y las que la ley excluye del principio genérico de notificación al domicilio ad litem (como la citación para absolver posiciones), deben practicarse en él. En determinados supuestos, es suplantado a estos fines por el domicilio legal, que según la definición del art. 90 del Código Civil es "el lugar donde la ley presume, sin admitir prueba en contra, que una persona reside de manera permanente para el ejercicio de sus derechos y cumplimiento de sus obligaciones, aunque de hecho no esté allí presente". Es el caso de las personas jurídicas en general, que la ley presume que residen para el ejercicio de sus derechos y obligaciones en el domicilio declarado en sus estatutos aprobados por la autoridad que les concedió la personería; y de los funcionarios públicos (que según el art. 90 inc 1º del Código Civil deben ser notificados en el domicilio legal, siendo este el lugar "en que deben llenar sus funciones, no siendo estas temporarias, periódicas o de 10 simple comisión"). En tercer lugar tenemos los domicilios especiales, que se eligen para la producción de ciertos efectos jurídicos en relaciones determinadas.

Así, las partes de un negocio jurídico pueden fijar un domicilio convencional como domicilio especial, que puede ser distinto del real, y pasa a ser el asiento legal de esa persona en cuanto a las obligaciones derivadas del contrato. Este domicilio convencional atribuye la jurisdicción y determina el lugar donde deben realizarse las notificaciones iniciales, incluso de la demanda (aunque no se extiende per se al proceso). Es decir que cuando existe un domicilio convencional o de elección, y se inicia un proceso judicial, éste sustituye al domicilio real. El segundo tipo de domicilio

especial relevante a los fines notificatorios es el domicilio procesal o ad litem o constituido, que debe fijar toda persona al intervenir en un juicio en su primera presentación. Pasa a ser el lugar donde las normas procesales establecen que se notificarán la gran mayoría de los actos sucesivos: es una garantía de la eficacia de la notificación. Se establece que debe ser dentro de un determinado perímetro o radio desde la sede del tribunal, de allí que requiera aprobación judicial. Mientras que la fijación de un domicilio convencional es voluntaria, la del procesal es una carga procesal obligatoria; y se diferencia del domicilio legal no sólo en que éste se rige por el derecho de fondo y aquel por el de forma, sino también en que el legal es de carácter general, mientras el domicilio ad litem es especial, solo rige para el proceso en cuestión. Cabe aclarar por último que la paralización por un tiempo prolongado del expediente provoca su invalidez.

4.1.2. La Digitalización de las Comunicaciones Judiciales: Alternativas

Luego de este brevísimo recorrido por las nociones jurídicas involucradas, corresponde analizar como pueden las tecnologías de la información y las comunicaciones aportar su potencial transformador al proceso de notificación. A nuestro entender, existen hoy tres variantes principales, que incluso pueden considerarse conceptualmente como sucesivas evoluciones de la misma idea, utilizar las TICs para dar mayor celeridad y eficiencia al proceso. Estas son:

- Suplantar las notificaciones por cédula en los casos que se realizan a un domicilio especial (convencional o procesal), por el envío de un correo electrónico a un domicilio electrónico especial (convencional o procesal).
- Suplantar las notificaciones por cédula en los casos que se realizan a un domicilio procesal, por su carga en un sitio web adonde la parte que debe notificarse puede, o no, acceder.

- Suplantar toda notificación automática o por cédula a un domicilio procesal por la mera publicación en Internet de la resolución, transformándolas en notificaciones automáticas.

Conste que en todos los casos hablamos de notificaciones por cédula a un domicilio especial (convencional o procesal), lo que excluye, en los casos que no se haya constituido un domicilio convencional, las notificaciones iniciales y las que la norma establece que deben ser al domicilio real. Lógicamente, casos como la notificación de la demanda deben seguir realizándose al domicilio real del demandado si no existe un domicilio convencional constituido ad hoc.

Vayamos a la primer variante. Para ella, es necesario que partes constituyan un "domicilio electrónico" especial (es decir, convencionalmente en un contrato o procesal, en su primera intervención en el juicio), en una dirección de correo electrónico, asumiendo la contraparte o el tribunal, a tal efecto, la obligación de emitir las notificaciones a esa dirección. Dado que resulta sencillo automatizar esta tarea en un sistema informático bien diseñado, no se recarga en modo alguno las labores de la oficina judicial si se asume que el tribunal sea quien emita automáticamente las notificaciones.

Por ejemplo hoy en día, con este sistema, la Cámara Laboral de Bariloche envía todas las notificaciones a la Caja Previsional, que responde del mismo modo, con gran ahorro de tiempo y de trabajo; y la utiliza el Dr. Toribio Sosa en Trenque Lauquen. Estas dos iniciativas tienen en común que requieren de la aceptación voluntaria de las partes para funcionar, y amparan su validez en el principio del saneamiento procesal ya descripto. Existen además otra serie de iniciativas como la que incluye a la firma digital en la provincia de Chubut, un proceso en marcha en Neuquén, y dos proyectos de acordadas de la Suprema Corte de la Prov de Bs As y del Superior Tribunal de Justicia de Río Negro. Cabe citar también por estar en pleno debate, una variación de esta propuesta, que es el ofrecimiento del Correo Argentino a la Suprema Corte de la Provincia de Buenos Aires para asumir las notificaciones dirigidas a domicilios procesales

constituídos, a testigos, peritos y otros auxiliares de la Justicia, las relacionadas con medidas cautelares y las que usualmente realiza la policía.

A través de un software utilizable en la PC de un abogado o de una dependencia judicial, se genera una cédula de notificación en formato digital, que una vez firmada digitalmente por el emisor, es transmitida electrónicamente a la oficina de Correo Argentino más cercana al domicilio del notificado. Allí, se imprimirá en papel de seguridad y será distribuido por personal del Correo Argentino. Concluido ese trámite, el comprobante se remite a la oficina judicial correspondiente. El personal privado tiene como fin imprimir las cédulas, entregarlas al destinatario, devolver los originales y generar información para la consulta electrónica en tiempo real del estado del trámite. De este modo, el Correo Argentino aprovecha que es el correo oficial de la Argentina y que puede dar fe postal. Este poder fedatario abarca el despacho, el contenido y la recepción de las comunicaciones fehacientes. Pero el circuito electrónico se reduce a una pequeña parte del proceso: el que va desde la oficina judicial hasta la oficina responsable de notificar; de allí hasta el destinatario, y luego de vuelta hasta la oficina judicial, el circuito sigue siendo físico. A todo evento, puestos a valorar la utilización de la firma digital como elemento adicional de seguridad en el proceso de notificación por correo electrónico, surge con claridad que, en la situación actual, con ella o sin ella estamos frente a un acto procesal irregular pero válido. Por tanto, al no estar normado su uso, y siendo que aporta complejidades tecnológicas, concluimos que no es indispensable su uso mientras no se regule normativamente. En el mismo sentido se ha expedido oficialmente la Cámara Laboral de Bariloche, lo cual reafirma que no es indispensable la firma digital a estos efectos, pudiendo utilizarse el correo electrónico simple.

La segunda variante, que propone cargar en un sitio web seguro las cédulas que deben notificarse al domicilio procesal, sitio web donde la parte que debe notificarse puede (o no) acceder, es el proyecto que está trabajando la Cámara Civil Nacional en la actualidad. A los letrados se les proporcionará un nombre de usuario y contraseña para acceder a un sitio web único (se planea extender la iniciativa a todos los fueros) donde

se les informará, discriminado por fuero, que cédulas ha recibido, en cuales expedientes ha sido notificado, y qué cédulas debe enviar. En una primer pantalla, el consultante sabrá que recibió, por ejemplo, 10 comunicaciones en un fuero y 10 en otro. Aun no está notificado, ya que no accedió a su contenido; pero tampoco sabe cuales son esas comunicaciones. Si desea conocerlas, accederá a una segunda pantalla, para un fuero, por ejemplo el Civil, donde sí verá el contenido de las notificaciones, discriminadas por juzgado y expedientes, quedando notificado en todas las del fuero, ya que accede de un modo identificado y no puede ver sino todas. De este modo, se piensa incentivar el uso del sistema, ya que el abogado puede tener interés en no notificarse en alguna causa, pero habrá otras en las que sí le importará la celeridad del trámite. Si pasado un cierto tiempo desde que se dispuso una notificación en el sitio, el abogado no accedió a notificarse, el sistema disparará una alarma y se lo notificará por el sistema tradicional. Esto significaría que en algunos casos (no se sabe cuantos) en definitiva el lapso que insume las notificaciones dentro del proceso se incrementará. Se prevé una primer fase optativa, en algunos juzgados piloto, para probar el sistema, antes de su difusión.

La tercer variante, que propone suplantar toda notificación automática o por cédula a un domicilio procesal por la mera publicación en Internet de la resolución, es la más audaz, y se basa en una premisa muy simple: un documento publicado en Internet está realmente a disposición de cualquiera, y mucho más de las partes en el juicio. Una vez recibida la notificación inicial, se presume que la persona que ha comparecido a estar a derecho debe, a partir de ese momento, seguir el trámite del proceso y asumir el riesgo procesal de su tramitación. Esta idea, muy propia de una creciente corriente de opinión en pro del activismo judicial en el área civil, puede sintetizarse citando una frase del Dr. Ariel Pelayo Labrada[36]: "si todos los proveídos salen diariamente por Internet, cabe entender que han tomado estado público, por lo que resulta innecesario otro tipo de notificación", de un modo incluso más sencillo (no hay que desplazarse físicamente hasta el juzgado) y amplio (en horarios y en posibilidad de obtener instantáneamente una copia en formato digital) que el acceso al expediente en el tribunal. Esta variante

[36] Pelayo Ariel Labrada, Diez claves para la celeridad procesal sin reformas legislativas, pág. 5, edición de autor, 2.000.

puede completarse con algún sistema de alarma automático que llegue al letrado a través del sistema informático, indicándole que ha habido un movimiento en determinado expediente. A diferencia de la notificación automática o ministerio legis en su estado actual, se trata de un acto expreso y no ficto de comunicación, dada la real disponibilidad de la información a través de Internet y su accesibilidad desde cualquier punto del planeta, a cualquier hora. Los obstáculos para su cumplimiento serían que el expediente no esté accesible (cosa absolutamente evitable, dado el elevadísimo grado de confiabilidad de los sistemas de información actuales), y que tal circunstancia se haga constar de algún modo. Es obvio que esta variante, para ser implementada, necesita de una reforma legislativa. Lo novedoso de esta iniciativa es que sigue los principios de la reingeniería de procesos, a saber:

- Buscar sistemáticamente, confrontar y criticar las hipótesis básicas implícitas en el proceso bajo análisis y probar a invertirlos o prescindir de ellos (en el centro de toda innovación reside el concepto de que hay que empezar el diseño del proceso sin encerrarnos en la manera de hacer de siempre).
- Intentar captar todo el poder de las nuevas TIC, ver qué permiten hacer y determinar cómo ayudan a replantear el proceso

  Para el caso de las notificaciones (tanto por cédula, como por edictos o ministerio legis), si probamos a prescindir de sus hipótesis básicas y los modos tradicionales, nos podemos plantear que la implementación del expediente digital accesible vía Internet ahorraría inclusive el paso de la notificación, muchas veces fuente de dilaciones inaceptables.

Sopesando las tres alternativas descriptas, podemos decir que la primera es la que concita en la actualidad más adhesiones y proyectos en marcha pues “replica” en el ámbito digital el procedimiento tradicional y puede implementarse sin necesidad de introducir reformas legislativas. La segunda ya hace pie en las características de acceso irrestricto y disponibilidad casi absoluta de la información publicada en Internet, pero queda a merced de la voluntad de los abogados de acceder o no a notificarse por esta vía; asumiendo que en caso contrario, los plazos de notificación serán más largos aun. A nuestro entender la tercera variante es el punto de llegada, hacia el que inexorablemente

se marcha, si bien con la dificultad de necesitar una adecuación legislativa de los códigos rituales.

Para reforzar el concepto de viabilidad respecto a lo que se propone, siguiendo en el campo de las comunicaciones, la consulta a terceros (hoy a través del diligenciamiento de oficios) puede beneficiarse notablemente aprovechando las nuevas tecnologías, en particular con los grandes proveedores o grandes fuentes de información relevante para la justicia. Así, ya hay tribunales no libran más oficios al Correo Argentino para cotejar si una carta documento efectivamente fue recibida o no en determinada fecha, sino que consultan esto directamente vía web, con gran economía procesal. Otro interesante antecedente es la circular del Banco Central que en 1998 ordenó que todos los pedidos de informes, embargos o inhibición de bienes que la Administración Federal de Ingresos Públicos (AFIP) dirigiera a los bancos se hicieran por medio de una página web. En primera instancia, los bancos procesaban esta información manualmente, aprovechando sólo parcialmente las posibilidades que brindaba la producción y publicación en formato digital de estos datos. Pero al decidirse a aprovechar integralmente las posibilidades, obtuvieron una notable reducción de costos. Por ejemplo, cuando en 1999 el Banque Nationale de Paris implementó una solución informática que compara las listas publicadas por la AFIP con una réplica de la base de clientes de la entidad (en formato Access), para verificar si las personas o entidades mencionadas por el organismo recaudador tienen cuentas en ese banco, que además "dispara" las contestaciones que correspondan de los oficios judiciales, obtuvo un ahorro de entre el 60 y el 80% del tiempo de trabajo de una persona, a un costo de sólo U$S 5.000.

Para terminar con los aportes comunicacionales de las nuevas tecnologías de la información a los procesos judiciales, mencionemos la cuestión de las comunicaciones interjurisdiccionales, de tribunal a tribunal, hoy regidas por la ley 22.172[37]. En diciembre de 2000 se celebró un seminario en la Junta Federal de Cortes, impulsado por el Programa Integral de Reforma Judicial del Ministerio de Justicia y Derechos Humanos, para el Uso de la Comunicación Electrónica Interjurisdiccional. En el mismo,

[37] infoleg.mecon.gov.ar/scripts1/.../cnsnorma.asp?tipo=Ley...22172

con la presencia de representantes técnicos de prácticamente todos los poderes judiciales y órganos extrapoder del país, se acordó un protocolo técnico para implementarlo, supeditado a un convenio al que adhirieron las Cortes y Superiores Tribunales. A nivel técnico, el convenio establece uniformar los nombres de dominio y la construcción de las direcciones de correo electrónico en los poderes judiciales (para facilitar el reconocimiento mutuo en las comunicaciones por email entre los tribunales, así como la identificación por la ciudadanía en general), e incorporar la firma digital a partir de la infraestructura existente en la Subsecretaría de la Gestión Pública, constituyéndose cada Poder Judicial como Autoridad de Registro para sus miembros. Ciertamente implicará no solo afianzar el funcionamiento de las redes informáticas sino también trabajar fuertemente con los jueces para que acepten esta nueva modalidad de comunicación.

Así, los tribunales de distinta jurisdicción quedan habilitados para comunicarse directamente por correo electrónico firmado digitalmente, con estilo informal, privilegiando la celeridad. El correo electrónico impreso se incorpora al expediente y basta como constancia actuarial.

4.2 ¿Por Dónde Empezar?

Cuando se toma conocimiento de nuevas prácticas utilizando herramientas tecnológicas, lo primero que pensamos es si ellas pueden contribuir a una mejora, y cómo podrían implementarse. Siguiendo la premisa de pensar en grande, comenzar en pequeño y crecer rápido; hemos visualizado el concepto de expediente electrónico con validez legal como objetivo a largo plazo, dentro del cual se encuentra obviamente el uso de firma digital de acuerdo a lo dispuesto en la Ley 25.506[38].

[38] infoleg.mecon.gov.ar/txtnorma/70749.htm

4.2.1. Etapa de Definición

A los efectos de generar cultura de uso de la firma digital, se comenzó a trabajar con aquellas comunicaciones no jurisdiccionales y de mero carácter administrativo. En tal sentido el PJN aprobó una reglamentación de doce artículos mediante la cual se disponía que determinado tipo de comunicaciones se dejaran de hacer en papel y se harían por correo electrónico. Para ello se utilizaron los certificados de firma digital emitidos por la Oficina Nacional de Tecnologías de Información (ONTI).

La reglamentación de las comunicaciones puede verse en el Anexo II (A) y la política de certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado puede verse en el Apéndice I.

La gestión de los certificados se realizaba a través de la Secretaría de Superintendencia, quien se había constituido en "Autoridad de Registro" (AR) de la ONTI, situación que permitía que la verificación de identidad del solicitante fuera realizada dentro del Poder Judicial. Las responsabilidades de la Secretaría de Superintendencia como AR (Decreto Nº 2628/02[39]) pueden verse en el Anexo II (B).

De acuerdo a lo establecido en la Decisión Administrativa Nº 6/7, y con referencia a los Oficiales de Registro que desempeñen funciones en la AR, se menciona que éstos deben proteger su par de claves, de manera que su clave privada se encuentre en todo momento bajo su exclusivo conocimiento y control, y con todas las medidas de seguridad establecidas por el certificador. Las condiciones para ser suscriptores de certificados emitidos así como el proceso de suscripción pueden verse en el Anexo II (C).

[39] infoleg.mecon.gov.ar/txtnorma/80733.htm

4.2.2. Utilización de la Firma Electrónica

Una vez generado el sustento técnico – administrativo descripto precedentemente, se comenzó a trabajar primero con la notificación de:

- Circulares: Son todas aquellas comunicaciones que emanan de la Secretaría de Superintendencia, relacionadas con directivas administrativas que el Tribunal Superior debe comunicar por cuestiones administrativas
- Decretos de presidencia: Resoluciones que toma el Presidente del Tribunal Superior como "Gerente" de la Organización
- Acuerdos Ordinarios del Tribunal Superior: Resoluciones que toma el Tribunal Superior (cuerpo colegiado) como "Directorio" de la Organización

Para ello se habilitó una casilla de correo por cada organismo susceptible de notificación, y reglamentariamente se designó un responsable de consultar dicha casilla una vez al día. En las notificaciones electrónicas se incluyó la leyenda:

"Dejo constancia, en mi carácter de Secretaria de Superintendencia, que el presente es testimonio del Original que se encuentra protocolizado.

Esta comunicación reemplaza la que se realiza en soporte papel y se encuentra firmado electrónicamente."

4.2.3. Siete Claves para Comenzar con una Iniciativa de Firma Electrónica

De la experiencia realizada surgen siete aspectos claves que no deben faltar en una iniciativa de este tipo:

- *Conseguir el patrocinio y compromiso del Directorio o Gerencia de la organización.* Resulta indispensable contar con este apoyo, dado el carácter de los cambios reglamentarios y de cultura de trabajo, que son necesarios para hacer útil y sostenible la utilización de medios electrónicos para reemplazar a objetos del mundo físico como es el papel.

- *Definir objetivos realistas y selección de la gente apropiada.* Un aspecto crítico en el proceso de definición de requerimientos es seleccionar un conjunto de éstos según los participantes relevados. Una definición válida de los objetivos y alcance permitirá centrarse en aquellos procesos en donde el uso de la firma electrónica será efectivo.

- *Su proceso debe ser visible antes de comenzar*. Como mencionábamos, la importancia de la visibilidad de los procesos en la iniciativa de SPI descripta en el Capitulo 3, aquí se pone de manifiesto la necesidad de contar con una reglamentación que asigne roles y responsabilidades para cada actividad involucrada.

- *Definir un criterio de evaluación y hacer el impacto visible*. Como en toda reingeniería de procesos, resulta muy conveniente tomar indicadores y medirlos, antes y después de la redefinición del proceso. En nuestro caso el 100% de los involucrados coincidieron en que el proceso era más rápido, más fiable y fácil de implementar. Las opiniones fueron recolectadas a través de un reporte ejecutivo y distribuido a distintos sectores de la organización y publicación en el portal web institucional, lo que permitió generar mayor interés por implementar esta práctica en otros procesos de notificación como aquellos relacionados con la administración de personal.

- *Promover el trabajo incremental y atento a la evolución*. Dividir las expectativas en diferentes piezas que se pueden integrar de forma

incremental es una práctica común, sin embargo encontrar el aporte fundamental trabajando de ésta manera no es tan fácil. Existen numerosas metodologías para ayudar a los administradores e ingenieros a seleccionar los requisitos básicos, y hay muchas recomendaciones procedentes del análisis de dominio, ingeniería de requisitos y análisis de negocio que nos dicen cómo empezar. A pesar del enfoque particular que se elija, es importante diferenciar las claves: un pensamiento evolutivo nos permite mantener el foco en el crecimiento sostenido en la aplicación de las diferentes facetas del proceso, prestando atención a los aspectos de riesgo que podrían obstaculizar el proyecto. Por otro lado, trabajar de forma incremental nos permite mostrar los primeros resultados, mantener a las personas involucradas a través de diseño de procesos participativos (por ejemplo, mediante la asignación de tareas específicas en cada incremento), y facilitar la documentación.

- *Generar documentación estándar y de fácil acceso*. Ya hemos mencionado que habíamos hecho la información visible a través de páginas web. Este hecho no necesariamente hace que la documentación sea de fácil acceso. Debemos realizar un cuidadoso diseño de los usos posibles, los perfiles interesados, estructura y organización de contenidos, y así sucesivamente. Además, las referencias a la documentación de apoyo deben ser previamente definidas. En nuestro caso, la ley provincial[40] fue la base para la definición de normas y procedimientos para el PJN. Después de eso, y mediante el análisis de las diversas necesidades, hemos definido un conjunto común de procedimientos para la utilización y la certificación de firmas electrónicas. Por ejemplo, hemos establecido claramente las responsabilidades y funciones. La clave fue diferenciar claramente las necesidades de los participantes y conceptualizar la información describiendo paso a paso los procedimientos. Finalmente, hacer que la información sea comprensible y de fácil acceso nos permitió generar más rápido una retroalimentación y evaluación, especialmente útil para nuestro caso

[40] http://www.jusneuquen.gov.ar/share/legislacion/leyes/leyes_provinciales/ley_2578.htm

piloto debido a la necesidad de demostrar que las firmas electrónicas son útiles en la Justicia.

- *Al menos un experto debe estar allí*. Es sumamente importante que el director del proyecto u otro experto con experiencia en ésta tecnología facilite el proceso de forma dinámica, guiando la iniciativa. El director de proyecto para un proyecto de firma electrónica debe tener suficiente autorización de la organización (que viene de su / cargo o como asesor) para llevar adelante el caso piloto. Una vez que los procesos son visibles y se establecen las metas, un equipo de implementación debe estar capacitados para llevar adelante la iniciativa. Este equipo va a ejecutar los procesos importantes, como la estandarización de normas y la definición de los canales de comunicación y puntos de control que requiere la firma electrónica. Estas actividades requieren una evaluación periódica y de apoyo para asegurar que los indicadores de proyecto y los resultados son los esperados. Aquí, un experto es el encargado de aclarar los objetivos, de la toma de decisiones en los procedimientos alternativos, y de evaluar en forma dinámica el impacto de los cambios introducidos.

  Para ello, él / ella debe ser capaz de establecer comunicación entre los distintos actores, desde políticos a técnicos. Esto significa que él / ella debe tener sólidos conocimientos de comunicación y de fondo sobre los dominios de gobierno. En nuestro caso, el papel de experto fue jugado por dos personas, que estaban a cargo de la ejecución del proyecto (como directores formales de proyecto). Sus antecedentes incluyen el conocimiento sobre el manejo de software y desarrollo de proyectos, el dominio del gobierno en el ámbito de la justicia, la mejora de procesos software, y la auditoría de calidad. Además, han gestionado los principales proyectos de software en el área de la justicia durante los últimos diez años.

4.3 Notificación Electrónica en el Ámbito Jurisdiccional

4.3.1. Inicio

Luego de la experiencia exitosa con el uso de la firma electrónica en notificaciones administrativas internas, ya habiendo generado la experiencia necesaria desde el punto de vista técnico y siguiendo los lineamientos dispuestos en el Plan Estratégico Informático 2010-2015 en lo referente a proyectos de e-gov, se comienza a trabajar en la puesta en marcha de notificaciones electrónicas en el ámbito jurisdiccional dentro de causas del fuero civil.

Nuevamente, bajo la premisa de pensar en grande, comenzar en pequeño y crecer rápido, se decidió que el alcance de este proyecto serían las notificaciones de 2 tipos de actuación judicial: interlocutorias y sentencias, en el ámbito de la Cámara Civil y las Secretarías del Tribunal Superior.

Como primera medida, y capitalizando la experiencia adquirida, se definieron las características deseables que debía tener el proceso de notificación:

- Definición del "domicilio electrónico", en donde el profesional recibirá la notificación, ya sea accediendo vía internet a un sistema provisto por el PJN o casilla de correo electrónico donde pueda visualizar las providencias que el Juzgado le notifica. Para la definición de este domicilio se deberá identificar a la persona a la cual se le asigna, lo que conlleva a la definición dentro del sistema de notificaciones, de un usuario y contraseña que trabaje con mecanismos de criptografía, que hagan a la misma invulnerable, siempre y cuando su propietario no la divulgue
- EL PJN debe asegurar toda la trazabilidad del proceso de notificación, llevando registros de auditoría de todas las notificaciones, que permitan conocer todos los estados por los que paso una notificación hasta que la misma fue "efectiva".

Todo ello a los fines de garantizar el correcto cumplimiento de la notificación sin tener que recurrir a servicios de terceros para acceder a dicha traza.

- El PJN debe asegurar con las herramientas tecnológicas existentes, la integridad del sistema de notificación, para que este se encuentre disponible y su información no sea adulterada. Para ello se utilizaran los llamados "protocolos seguros" de comunicaciones, que se establecerán entre los Letrados y el PJN a través de internet, estos protocolos tienen la característica de cifrar la información transmitida para que la misma no sufra modificaciones o adulteraciones en su transmisión

4.3.2. Gestión de Riesgos para la Implementación de Notificación Electrónica

Así mismo se llevó adelante una gestión de riesgos para garantizar que las notificaciones no incurran en una nulidad del acto jurídico por cuestiones de índole técnico. En tal sentido se definieron los siguientes riesgos y su estrategia de mitigación:

- *Interrupción del servicio de correo electrónico*: La infraestructura tecnológica debe diseñarse tolerante a fallos, desde el punto de vista del servidor de correo electrónico así como de las comunicaciones, especialmente debe elegirse un ISP (internet service provider) que asegure una disponibilidad de servicio mayor al 95 %.
- *Resistencia al cambio por parte de los abogados*: Según sea el contenido de la notificación, existe la posibilidad de que la estrategia legal del abogado sea dilatar al proceso judicial, en cuyo caso le conviene que las notificaciones sean lentas. Para este caso debe involucrarse a los Colegios de Abogados comprometiéndoles como parte del proyecto, para mitigar la resistencia que puede existir entre sus matriculados.
- *Resistencia a la iniciativa porque a los abogados se le acortan los plazos para actuar a partir de las notificaciones*: Normalmente gracias al sistema de

procuración electrónica desarrollado por el Poder Judicial, los abogados cuentan con la información que se les va a notificar entre 7 y 10 días antes de que sean notificados legalmente, esto les reporta un mayor margen para actuar. Con la iniciativa de notificación electrónica este margen disminuye sensiblemente, por lo que se advirtió que podría haber una seria oposición a la implementación de este tipo de notificaciones. Para mitigar este riesgo el PJN dispuso que los plazos legales comenzaran a correr luego del tercer día a partir de que el abogado recibió la notificación en su casilla electrónica.

- *Que el abogado cuestione o niegue la recepción del correo electrónico*: Para evitar este riesgo, el PJN dispuso la asignación de una casilla de correo a cada profesional para notificaciones. Tomando el certificado de entrega de correo que emita el servidor de correo electrónico como comprobante de que la notificación se realizó correctamente.

4.3.3. Implementación

Una vez definidas las características deseables de la implementación y la resolución de los riesgos de mayor impacto existentes se comenzó a delinear la solución a implementar.

Esta solución debía contemplar cómo hacer para que el sistema de correo electrónico pueda interactuar con el sistema de gestión judicial existente (legacy), dado que como se trataba de una experiencia piloto no se definió cambiar el software hasta tanto no se tenga experiencia en el uso de esta herramienta en el ámbito jurisdiccional, ya que a partir de ello seguramente irían surgiendo ajustes al procedimiento de notificación. Esta interacción entonces se ve reflejada en el esquema conceptual de la Figura 15.

El esquema general funciona de la siguiente manera: Cuando llega una orden de notificación (1), se procesa mediante procedimientos adicionales a los componentes del sistema de gestión manejados por los componentes "wrapper", que están a cargo de la normalización y el llenado de la información. Entonces, la

notificación es firmada electrónicamente (2). Para ello, hemos desarrollado un conjunto de regulaciones sobre el uso de firma electrónica, junto con un manual que detalla el conjunto de procesos y documentos relacionados. El reglamento se compone de 12 artículos que declaran el alcance, las autoridades (incluidas las autoridades de registro) y el conjunto de leyes y documentos sobre los cuales se construyen las regulaciones (ver Anexo II). Para llevar a cabo la notificación de actuaciones, como mencionábamos anteriormente las partes interesadas (empleados del sistema judicial) deben tener la firma electrónica, llamando a cada uno de ellos un "suscriptor". Cada suscriptor es responsable de la utilización de su /certificado identificado con una clave privada, que es secreta e intransferible.

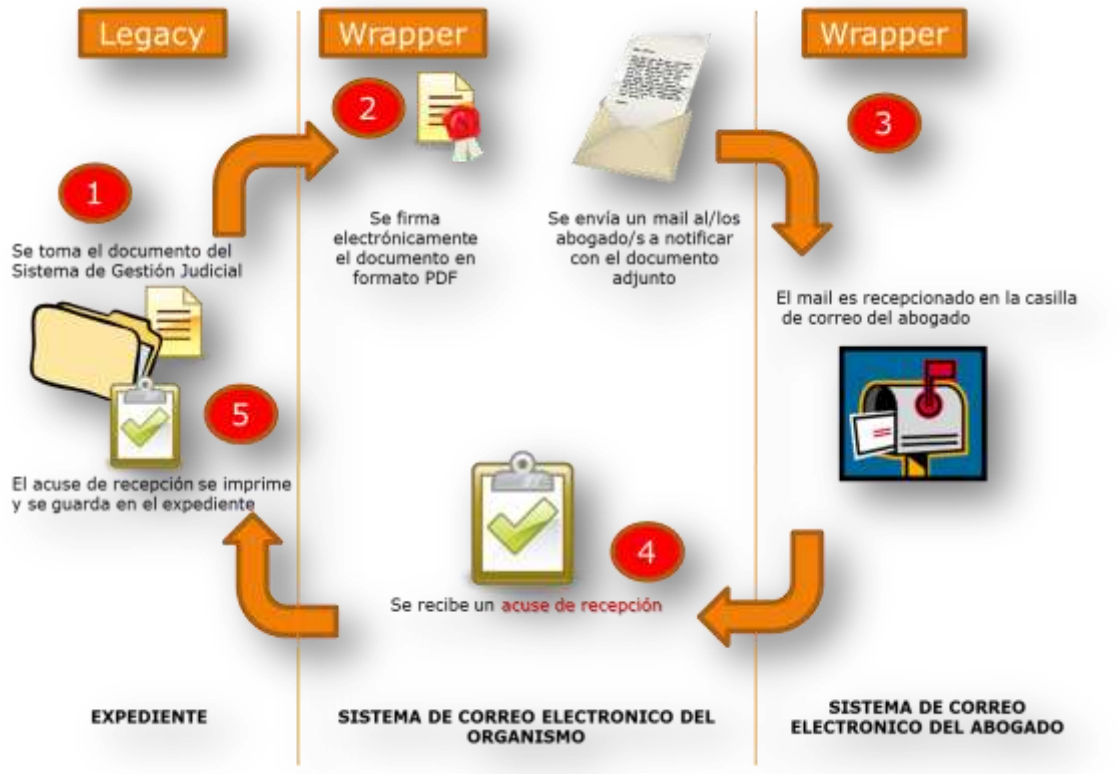


Figura 15. Esquema Conceptual del Procedimiento de Notificación

Después de firmar la notificación, se envía al abogado (representante del actor/demandado) correspondiente (3) a través de un servidor de correo

tradicional. El detalle importante aquí es que las cuentas de correo electrónico son proporcionadas por el Poder Judicial durante la fase de adhesión al servicio de notificación electrónica. En otras palabras, la cuenta de correo electrónico para las notificaciones es creado y administrado por el Sistema Judicial (no es posible el uso personal o privado de la cuenta de correo electrónico). Un acuse de recibo emitido por el servidor de correo se recibe tan pronto como el e-mail es puesto en la casilla de correo del abogado a notificar (4). Este acuse de recibo se incorpora en el Sistema de gestión judicial y en el expediente en papel (5) para mantener una versión impresa.

El propósito de este esquema es definir las limitaciones y los flujos de control que deben existir para implementar la notificación electrónica de manera que el mismo sea eficiente.

Figura 16. Notificaciones Electrónicas en la Cámara Civil

En la Figura 16 podemos ver el esquema de cómo se desarrollan las notificaciones electrónicas en la Camara Civil. Después de llegar a una sentencia sobre un caso, la que esta representada por un nuevo documento en papel, se genera una orden de notificación (1). Se ingresa en el sistema de gestión judicial (SGJ), que se dividió en dos tipos principales de componentes: el sistema "legacy" y el wrapper. La Secretaría de Informática esta a cargo de la gestión de los procedimientos para la normalización de los documentos de acuerdo con las normas establecidas para la firma electrónica. El SGJ permite gestionar y producir información de los casos a través de la simplificación de tareas administrativas a causa de los textos y documentos estandarizados. Evita esfuerzos innecesarios causados por las tareas duplicadas y sin valor agregado, y permite el acceso fácil y rápido de los casos a través de un sistema basado en Internet. Esta aplicación fue desarrollada con una arquitectura cliente-servidor utilizando Lotus Notes y Domino, y la integración de la plataforma se realizó con herramientas de colaboración (correo electrónico, agenda, etc.).

Los documentos se almacenan en un servidor de notificaciones (NotifyServer), que es un componente particular diseñado para mantener el estado de la notificación. A continuación, se solicita una firma electrónica (2) lo que luego se traducirá en un documento compuesto por una combinación de información de texto que detalla la naturaleza de la solicitud, y una identificación electrónica a través de una firma electrónica válida. De esta forma, el contenido del documento está "congelado", por lo que cualquier alteración invalida la firma electrónica. Este proceso utiliza un método de cifrado, que implica el uso de algoritmos de clave asimétrica, es decir, la información no- mensaje es necesaria para transformar el mensaje de una forma segura, y es diferente de la información necesaria para revertir el proceso. Cuando alguien quiere enviar un mensaje seguro, el emisor lo encripta (lo transforma para asegurar la forma) con la clave privada del destinatario; para descifrar el mensaje, el destinatario utiliza la clave pública. Nuestro método particular tiene tres propiedades interesantes: longitud de un mensaje fijo en forma independiente de la longitud del documento, una mínima alteración del documento produce grandes variaciones del mensaje, y el cálculo no es simétrico, luego no es posible usarlo para volver a descifrar el documento.

Por último, el abogado recibe la notificación firmada (3) en la cuenta de correo electrónico provista por el Poder Judicial y el estado de la notificación se actualiza en consecuencia. Para finalizar el proceso (4) (5), se imprime un acuse de recibo de la notificación, se añade al expediente en papel, y se da de alta un documento en el SGJ indicando que la notificación se cursó exitosamente.

4.3.3.1. Guía de Implementación

Nuestra experiencia en la implementación de las notificaciones electrónicas dentro del ámbito jurisdiccional del fuero civil, nos deja como lecciones aprendidas, siete puntos clave que debieran abordarse en una iniciativa de éste tipo:

1. Gestione la aceptación de todas las partes involucradas, a través de una eficaz comunicación de los beneficios que obtiene cada una de ellas, con gran énfasis en el bien común y beneficio de los justiciables (ciudadanos que requieren del servicio de justicia).
2. Conforme un equipo de trabajo multidisciplinario con un líder de proyecto que tenga formación en TICs (Tecnologías de Información y Comunicaciones) y domine el conocimiento del área de aplicación, jueces o secretarios (funcionario que firma las notificaciones) que usarán el nuevo sistema de notificación electrónica, y un representante directo del PJN.
3. Difunda el plan entre los actores internos de la organización y escuche sus opiniones para hacer los ajustes correspondientes. Si aplica sus recomendaciones hágaselo saber, eso redundará en contar con aliados al momento de la implementación.
4. Difunda el Plan entre los actores externos (abogados), convóquelos a través de su colegio profesional, busque sus opiniones para validar su plan y la solución diseñada. Involúcrelos a través de su colegio profesional; si aplica sus recomendaciones hágaselo saber, al igual que con los actores internos esto redundará en contar con aliados al momento de la implementación.

5. Elija una plataforma tecnológica lo más sólida posible o lo mejor que su presupuesto pueda pagar. Si no la tiene, sume los especialistas en TICs para mantener proactivamente la plataforma tecnológica. Gestione anualmente un presupuesto acorde para cumplir con éste mantenimiento.
6. La seguridad que no pueda darle la tecnología a la cual tiene acceso, compénsela con la redacción de planes de contingencia por si ésta falla. Los actores deben percibir solidez en el cambio, dicha solidez debe despejar las dudas que éstos tengan ante posibles fallos.
7. Defina e implemente un servicio de "Mesa de ayudas" para asistir a los actores externos e internos con los problemas o dudas que se les puedan presentar.

Como puede observarse estas recomendaciones abordan puntos clave para generar confianza y disipar la incertidumbre respecto al cambio en la modalidad de notificación, que elimina un objeto físico como lo es la "cedula de notificación impresa en papel" que los abogados han utilizado durante décadas, en tal sentido se definió como condición necesaria abordar todas la inquietudes planteadas por los letrados, a los efectos de dar certidumbre de cómo se procedería en los casos que por razones técnicas el sistema saliera de servicio o las garantías de certificación de la entrega sin alteración de la notificación.

4.3.4. Análisis de Resultados

Entre los beneficios que se obtienen a partir de la implementación de la notificación electrónica se pueden mencionar:

- Reducción de costos:
    - El proceso manual para una notificación involucra la intervención de 6 personas, mientras que para la notificación electrónica intervienen 2.
    - Los costos en insumos por notificación son mayores en el proceso manual, considerando el riesgo de accidentes que pueden sufrir el

notificador cuando se traslada en automóvil hacia el domicilio en donde debe dejar la notificación.

- Cuando existen problemas para encontrar el domicilio o a quien reciba la notificación, el notificador debe volver al menos 2 veces.

- Reducción en los tiempos de notificación: 1 día para la notificación electrónica vs 7 días para la manual.
- Menor riesgo laboral para los trabajadores: intervienen menos personas en el proceso, y las mismas no están expuestas a los accidentes que puedan sufrir en la vía pública.
- No hay riesgo de extravío de las notificaciones: En el proceso tradicional existe el riesgo de extravío de papeles, debido al gran volumen que se maneja.
- Mejora en el servicio de justicia: A partir de la reducción en la duración del proceso judicial, y mayor efectividad en la actividad de notificar.

Hemos prestado especial atención a los efectos secundarios y a manejar el impacto de los cambios dentro de la organización. En la actualidad, los procedimientos de notificación electrónica se institucionalizan y se utilizan para comunicar las sentencias varios de los casos con un alto nivel de aceptación. No sólo la seguridad ha mejorado, sino también la visibilidad y la transparencia del proceso de notificación. Estos resultados son promisorios y nos dan la posibilidad de ampliar el apoyo al proyecto estratégico de gobierno electrónico.

5. CONCLUSIONES

En el presente trabajo se ha abordado la temática de la mejora de procesos, estándares de calidad y gobierno electrónico, mostrando en primer lugar el estado del arte de las mencionadas temáticas, para luego enfocarnos en los requisitos, con sus restricciones, que demandaba una institución como el Poder Judicial de Neuquén, como caso de estudio, para poder llevar adelante un programa de gobierno electrónico que sea exitoso y sustentable en el tiempo. Se ha hecho énfasis en la mejora de procesos y calidad del software para asegurar que las herramientas de software que se construyeran para implementar funcionalidades de e-gov fueran robustas, producto de un proceso establecido, visible y trazable. Esto se definió así dado que en una organización tan tradicionalista y conservadora, no estaría predispuesta a convivir con funcionamientos defectuosos de herramientas tecnológicas dentro del proceso judicial; es decir que si cambiábamos algo en el proceso judicial, éste cambio debía fundarse sobre una hipótesis de mejora que luego debía demostrarse en la realidad.

Las iniciativas de gobierno electrónico presentadas en este trabajo, son las primeras que afectan al proceso de causas judiciales, y se les ha dado validez legal poniendo de manifiesto lo acertado de su diseño, independientemente de otras soluciones que puedan existir para la problemática expuesta.

A continuación se analizan los resultados del trabajo llevado a cabo en esta tesis. De esta manera, los apartados incluidos son los siguientes: análisis de la consecución de objetivos, principales aportes de esta tesis, contraste de los mismos en publicaciones científícas y líneas de trabajo abiertas.

5.3. Análisis de la Consecución de Objetivos

En el primer capítulo de esta tesis se han presentado los objetivos parciales que se pretendían cumplir para satisfacer el objetivo principal de nuestra investigación, que es el siguiente:

Desarrollar guías y experiencias para la aplicación de mejora de procesos en ámbitos gubernamentales que sirvan de soporte a la inclusión de prácticas de gobierno electrónico.

A continuación se presenta una valoración de la consecución de cada uno de los objetivos parciales:

- Objetivo A: *Proponer guías de para la aplicación de mejora de procesos en el marco de organizaciones gubernamentales*.

  Hemos analizado la relación existente entre mejora de procesos software y gobierno electrónico en el contexto citado por diversos autores y como plataforma base para el emprendimiento de una acción sostenida en pro de la prestación de servicios efectivos al ciudadano. En el Capítulo 2 hemos enfocado específcamente en la propuesta del uso de modelos de mejora de procesos software, y en particular en el modelo CompetiSoft, como vehículos para introducir calidad y visibilidad a los procesos de desarrollo de software. También hemos analizado las contribuciones de la mejora de procesos al gobierno electrónico (Sección 2.3). Usando esta base conceptual y las lecciones aprendidas de los casos de estudio descriptos en el Capítulo 3, hemos detallado beneficios y dificultades, y hemos establecido un marco incremental como guía para lograr mayor visibilidad en los procesos.

- Objetivo B: *Establecer relaciones entre las guías para la aplicación de mejora de procesos y la inclusión de prácticas de gobierno electrónico – en particular firma electrónica.*

  La mejora de procesos ha sustentado la posibilidad de arribar a aplicaciones de prácticas de gobierno electrónico que han resultado exitosas. Las lecciones, guías y recomendaciones reflejan con claridad las relaciones establecidas (Sección 4.2.3, Sección 4.3.2). Por otra parte, la descripción de pasos a seguir para la inclusión de las prácticas, ha revelado que institucionalizar los procesos

de firma y notificación electrónica ha mejorado no sólo la seguridad sin también la visibilidad y transparencia de esos procesos (Sección 4.2, Sección 4.3).

- Objetivo C: *Validar la propuesta en caso de estudios reales analizando lecciones aprendidas.*

  A partir de la base conceptual resumida en el Capítulo 2, hemos realizado un caso de estudio en el dominio del Poder Judicial de la Provincia de Neuquén adhiriendo a su Plan Estratégico (Capítulo 3). El caso de estudio se ha circunscripto a la aplicación mejora de procesos en dos pilares fundamentales: la gestión de recursos para los proyectos (Sección 3.1.1) y la definición y fortalecimiento de la estructura encargada de dar soporte al usuario (Sección 3.1.2). En cada caso, se han detallado los pasos llevados a cabo y se han analizado resultados en base a diversos indicadores.

  La inclusión de prácticas de gobierno electrónico (firma y notificación) se ha realizado en el mismo dominio, estableciéndose procesos para la implantación así como guías de implementación. El Capítulo 4 describe estos casos en detalle.

5.4. Principales Aportaciones

Como principales aportes de esta tesis se pueden mencionar los siguientes:

- Un estudio conceptual sobre relaciones entre mejora de procesos software e introducción de prácticas de gobierno electrónico.
- Un conjunto de guías, recomendaciones y lecciones aprendidas derivadas de casos de estudio que enfocaron dos aspectos: la mejora de procesos en sí misma y la inclusión de prácticas de gobierno enmarcadas en un proyecto integral basado en aumentar la calidad y visibilidad de esos procesos.

5.5. Contrastación de Resultados

A continuación se detallan las publicaciones realizadas hasta el momento de resultados parciales de esta tesis. Las mismas se listan clasificadas según su tipo:

Capítulos en Libros

- Juan M. Luzuriaga, Rodolfo Martínez, Alejandra Cechich, Capítulo: *Improving Resource Management: Lessons from a Case Study from a Middle-Range Governmental Organization*, En: Software Process Improvement for Small and Medium Enterprises: Techniques and Case Studies Editado por Hanna Oktaba, Mario Piattini ISBN 978-1-59904-906-9 Editorial: IGI Global Publishing Páginas: 327—341 Año: 2008

Conferencias Internacionales

- J. Luzuriaga, A. Cechich. Artículo: *Electronic Notification of Court Documents: A Case Study*. En Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance. Editorial: ACM (Association for Computing Machinery) Lugar de edición: USA. A ser publicado Septiembre 2011.
- J. Luzuriaga, R. Martínez, A. Cechich. Artículo: *Design and Implementation of an Electronic Signature Solution in the Justice Area*. En Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance Editado por: Tomasz Janowski & Jim Davies ISBN 978-1-60558-663-2 Editorial: ACM (Association for Computing Machinery), Páginas: 299-304 Año: 2009.
- Juan M. Luzuriaga, Rodolfo Martinez, Alejandra Cechich Artículo: *Setting SPI Practices in Latin America: An Exploratory Case Study in the Justice Area* En: Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance. Editado por: Tomasz Janowski, Theresa A. Pardo ISBN 978-1-60558-386-0 Editorial: ACM Press, Páginas: 172—177 Año: 2008

Conferencias Nacionales

- J. M. Luzuriaga, R. Martínez, A. Cechich. *Mejora en la Gestión de Recursos: Experiencias hacia la Aplicación de un Estándar Ibero Americano*. 7° Argentine Symposium on Software Engineering (ASSE), 35 JAIIO, Mendoza, 4-8 Septiembre, 2006.

5.6. Trabajos Futuros

El trabajo presentado en esta tesis ha enfocado algunos aspectos concernientes a la relación entre Tecnologías de la Información y Comunicaciones y la introducción de prácticas de gobierno electrónico – en particular la sinergia que puede establecerse al incorporar Mejora de Procesos Software como mecanismo para brindar un soporte al e-gov. Sin embargo, la madurez de una organización en cuanto a la inclusión de prácticas de gobierno electrónico no sólo se relaciona con mejora de procesos. Los denominados "modelos de madurez" tienen el propósito de proporcionar marcos de referencia sistemáticos para evaluar el desempeño de las organizaciones en determinadas áreas de actuación, así como mapas de ruta para mejorarlo mediante la especificación de posibles niveles de evolución.

Surge entonces, la necesidad de medir y evaluar el grado de preparación que tienen las instituciones públicas, para dar cumplimiento a las nuevas directrices nacionales en torno al gobierno electrónico y en general para abordar los nuevos desafíos que impone el enfoque e-gov de administración publica. Es decir, la aplicación de un modelo de madurez y capacidad de e-gov, que bajo un enfoque multidimensional y holístico integre la evaluación de capacidades tecnológicas, organizacionales, operacionales y de capital humano, y que permita al gobierno evaluar el grado de preparación de los servicios públicos.

Aunque existen diversos esfuerzos por establecer un modelo de madurez de e-gov [4][41] la madurez organizacional involucra factores complejos – cognitivos, técnicos, de infraestructura, etc., que pueden establecer esquemas estructurales difíciles de ser abordados.

Una interesante línea de trabajo futuro consiste en explotar las lecciones aprendidas en este trabajo de tesis como base para el estudio, integración y evaluación de factores organzacionales como soporte a prácticas de e-gov.

ANEXO I – TEST MYERS-BRIGGS (MBTI)

Tilde aquellas opciones que reflejen algún aspecto de su personalidad o se identifiquen con parámetros de acción ante las diferentes situaciones que se plantean.

☐ Tiende a hablar primero, pensar después y no sabe qué decir hasta que Ud. se escuche diciéndolo; con frecuencia se regaña así mismo con cosas como "aprenderé alguna vez a mantener mi boca cerrada"

☐ Conoce mucha gente y a muchos de ellos los considera como amigos íntimos; le gusta incluir tanta gente como sea posible en sus actividades.

☐ No le importa leer o tener una conversación mientras se desarrolla otra actividad simultáneamente (como una conversación, la tv. Radio, etc.); en realidad puede permanecer indiferente a esta distracción.

☐ Le gusta ir a reuniones y tiende a manifestar su opinión; en realidad se siente frustrado si no le dan la oportunidad de expresar su punto de vista.

☐ Prefiere generar ideas en un grupo que por su cuenta; se siente agotado si pasa mucho tiempo reflexionando sin tener la oportunidad de intercambiar sus ideas con otros.

☐ Disfruta de la paz y la tranquilidad de tener tiempo para Ud. mismo; halla que su tiempo privado se encuentra fácilmente invadido y tiende a adaptarse desarrollando un alto poder de concentración que le permite aislarse de conversaciones cercanas, teléfonos sonando y otros similares.

☐ A veces lo han calificado de tímido; esté o no de acuerdo, puede impresionar a otros como alguien reservado y pensativo.

☐ Le gusta compartir ocasiones especiales sólo con alguna otra persona o quizás con algunos amigos íntimos.

☐ Desearía imponer sus ideas con más fuerza. Le molesta que otros digan antes cosas que Ud. estaba por decir.

☐ Sus padres le decían cuando era chico, andá afuera a jugar con tus amigos; sus padres quizás se preocupaban porque Ud. prefería jugar solo.

☐ Prefiere respuestas específicas a preguntas específicas; cuando pregunta la hora, prefiere que le digan 3:32, le molesta que le digan falta un poco para las 4 o es hora de

ir.

☐ Le gusta concentrarse en lo que está haciendo en ese momento y generalmente no le preocupa lo que sigue; es más, prefiere hacer algo que pensar en ello.

☐ Encuentra más satisfactorios aquellos trabajos que producen resultados tangibles; aunque le disguste el trabajo de la casa, preferiría limpiar su escritorio a pensar que le depara el futuro de su carrera.

☐ Prefiere resultados con hechos y números que con ideas y teorías; prefiere escuchar las cosas en forma secuencial en lugar de al azar.

☐ Se siente frustrado cuando las personas le dan instrucciones poco claras o cuando alguien le dice "este es el plan general", nos ocuparemos de los detalles después; o cuando Ud. escucha instrucciones muy claras y otros las tratan como si fueran lineamientos vagos.

☐ Piensa en varias cosas al mismo tiempo; a menudo sus amigos y colegas lo señalan que está "como ausente".

☐ Cree que hablar de detalles aburridos es una redundancia.

☐ Cree que el tiempo es relativo; no importa la hora a menos que la reunión, cena o evento haya comenzado sin Ud.

☐ Encuentra más atractivo buscar las relaciones y conexiones subyacentes a las cosas, más que aceptarlas tal como aparecen; siempre está preguntando qué es lo que eso significa.

☐ Tiende a dar respuestas generales a las preguntas; no comprende por qué tanta gente no puede seguir sus instrucciones y se irrita cuando la gente lo presiona en busca de especificaciones.

☐ Es capaz de mantenerse frío calmado y objetivo en situaciones donde todo el mundo está alterado.

☐ Preferiría resolver una disputa basándose en lo que es justo y verdadero más que en lo que hace a la gente feliz.

☐ Le gusta demostrar su punto de vista por motivos de claridad; es habitual en Ud. discutir ambos puntos de vista en un debate simplemente para ampliar su horizonte intelectual.

☐ Es una persona de ideas firmes que uno de corazón tierno; si Ud. está en desacuerdo con las personas prefiere decírselos que a callar y que crean que está de acuerdo.

☐ Se enorgullece de su objetividad -a pesar del hecho de que algunos lo acusan de ser frío e indiferente- si Ud. sabe que no puede estar más alejado de la verdad.

☐ Considera como una buena decisión la que toma en cuenta los sentimientos de otros.

☐ Se extralimita tratando de satisfacer las necesidades de otros; hará casi cualquier cosa para acomodar a otros incluso a expensas de su propio confort.

☐ Se pone en el lugar de los demás; Ud. es quien en una reunión probablemente pregunte como afectará esto a la gente involucrada.

☐ Disfruta dando servicios necesarios a la gente aunque algunos se aprovechen de Ud.

☐ A menudo se pregunta si alguien se preocupa por lo que Ud. desea aunque tenga dificultad en decírselo a alguien.

☐ Siempre espera a otros, quienes nunca parecen ser puntuales.

☐ Tiene un lugar para cada cosa y no se siente satisfecho hasta que cada cosa esté en su sitio.

☐ Se despierta por la mañana y sabe bastante bien como será su día; tiene una agenda armada y la sigue y puede llegar a ponerse alterado si las cosas no marchan como estaba planeado.

☐ No le gustan las sorpresas y esto se lo hace saber a los demás.

☐ Le deleita el orden; tiene su manera especial para guardar las cosas en su escritorio, en sus archivos o para colgar cosas en las paredes.

☐ Se distrae fácilmente; se "pierde" en el camino de la puerta de calle al auto.

☐ No planifica una tarea hasta ver que es lo que se requiere; la gente lo acusa de ser desorganizado aunque Ud. sabe mejor que es lo que hay que hacer.

☐ No cree que la prolijidad sea importante, aunque preferiria tener las cosas en orden; lo importante es la creatividad, la espontaneidad y la capacidad de respuesta.

☐ Convierte todo trabajo en una diversión; si un trabajo no puede ser algo entretenido probablemente no sea digno de hacerse.

☐ No le gusta que le obliguen a tomar decisiones ; prefiere mantener sus opciones abiertas.

ANEXO II – REGLAMENTACIONES

A) Comunicaciones

Artículo 1. Objeto. Se dispone dentro del ámbito del Poder Judicial, la utilización de la firma electrónica y su eficacia en las condiciones que se establecen en el presente reglamento.

Artículo 2. El órgano de aplicación de la firma electrónica es el Poder Judicial de la Provincia del Neuquén.

Ámbito del registro: para actuar dentro del ámbito del poder judicial, se designa como organismo de registro a la Secretaría de Gestión Humana y Programas Especiales y a la Secretaría de Superintendencia ambas del Tribunal Superior de Justicia. *Autoridades de registro:* Designase como autoridades de registro -para actuar dentro del ámbito del Poder Judicial- , al titular de la Secretaría de Gestión Humana y Programas Especiales y a la Secretaría de Superintendencia ambas del Tribunal Superior de Justicia.

Artículo 3. Las autoridades actuantes -Secretaria de Superintendencia y la Secretaria de Gestión Humana del Tribunal Superior de Justicia- elaborarán los procedimientos que implementen las políticas que surjan del uso de la firma electrónica.

Asimismo, serán los organismos encargados de proponer las modificaciones que se requieran en la presente reglamentación en función de las modificaciones legislativas que pudieran producirse teniendo en cuenta lo que dispone el art. 4 del presente. Dictará los instructivos y manuales necesarios para el uso de la herramienta “firma electrónica”.

Artículo 4. A los fines de este reglamento, se toman en consideración los siguientes instrumentos, que integran la presente reglamentación:

a. Ley provincial 2.578

b. Ley nacional 25.506

c. Decreto reglamentario 2628/02 y sus modificatorios

d. Decreto 283/03[41]

e. Documento de política de certificación de la autoridad certificante (Punto 2 inc.c dispone que resulta de aplicación a los suscriptores)

f. Normativa que en su consecuencia se dicte tanto en el orden nacional, como provincial.

Mientras que en sus consideraciones particulares se disponía:

Artículo 4. Dispónese la utilización de la firma electrónica, en todas las comunicaciones internas del Poder Judicial. Tanto las que impliquen transmisión de información relacionados con licencias –con excepción de la prevista en el art. 14 del Reglamento de licencias vigente- como las comunicaciones interorgánicas de carácter administrativo que surgen del manual de procedimientos.

Artículo 5. Cada titular de juzgado y su secretario – para el caso de órganos jurisdiccionales-; titular y adjunto de ministerios públicos – para el caso de organismos del Ministerio Público fiscal y pupilar; y jefes de organismos y sus respectivos jefes de área, de departamento y/o subsecretarios - para los casos de los demás organismos administrativos-, contarán con firma electrónica.
Se denomina a cada usuario "suscriptor o titular de certificado digital". Cada suscriptor de certificado, es responsable por su utilización. Este debe ser exclusivamente para documentos emitidos para ser utilizados dentro del Poder Judicial. La clave es única, secreta e intransferible (Conf. punto 5.6 del documento 'política de certificación') Se considerará falta grave la falta de resguardo, divulgación y/o incorrecta utilización de la firma electrónica. El suscriptor o titular aludido precedentemente quedará notificado al momento de serle entregado el certificado digital, del presente reglamento y la normativa que forma parte integrante del mismo.

Artículo 6. Dentro de la gestión del organismo, cada titular podrá designar un responsable, que en principio debe ser el prosecretario del organismo, o el jefe de departamento, Jefe de despacho y/o cualquier otro personal idóneo que el titular determine, para la confección, manejo y resguardo de los correos que se hayan firmado

[41] infoleg.mecon.gov.ar/txtnorma/82362.htm

electrónicamente.Dicho responsable será el encargado de llevar un registro y archivo de los mismos mediante el uso de carpetas.

Artículo 7. El responsable aludido en el artículo que antecede será además, el encargado de revisar diariamente la casilla de correo electrónico institucional del organismo.
Cuando se verifique la recepción de un email, firmado electrónicamente, comunicará la circunstancia al actuario, debiendo imprimirse el documento y notificarse al/los destinatarios del mismo.

Artículo 8. Es obligatorio revisar diariamente las casillas de correo electrónico institucionales, tanto las personales como las del organismo.

Artículo 9. La fecha de notificación de la documentación emitida mediante el uso de la tecnología electrónica, será la fecha en que el mail ingrese al servidor de correo electrónico.

Artículo 10. Desde la Secretaría de Informática, se configurará el equipamiento existente en los casos que sea necesario, quedando expresamente prohibida la instalación de programas o cualquier tipo de software en el equipamiento del Poder Judicial, que interfiera con la normal ejecución de los sistemas de uso de la gestión judicial, que incluye los organismos administrativos.

Artículo 11. Los mecanismos de utilización, modelos de documentos y demás cuestiones inherentes se elaborarán dentro del marco del manual de procedimientos que se elaborará por las autoridades de registro debiendo efectuarse cualquier consulta a las secretarías de Superintendencia y de Gestión Humana del Tribunal Superior de Justicia.

Artículo 12. Las autoridades de registro elaborarán el listado de magistrados y funcionarios que serán titulares de certificados digitales, poniendo en conocimiento del cuerpo los mismos.

B) Responsablidades de la Autoridad de Registro

a) Recibir las solicitudes de emisión de certificados.

b) Validar la identidad y autenticación de los datos de los titulares de certificados.

c) Validar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador.

d) Remitir las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) Recibir y validar las solicitudes de revocación de certificados y su direccionamiento a la AC ONTI.

f) Identificar y autenticar los solicitantes de revocación de certificados.

g) Archivar y conservar toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) Cumplir las normas y recaudos establecidos para la protección de datos personales.

i) Cumplir las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador con el que se encuentre vinculada, en la parte que resulte aplicable.

C) Condiciones para ser suscriptores de certificados y proceso de solicitud

En tal sentido podrán ser suscriptores de los certificados emitidos por la AC ONTI los funcionarios y agentes públicos y las personas contratadas bajo cualquier modalidad de contratación que desempeñen funciones en los organismos y entidades del Sector Público o bien, los funcionarios y agentes públicos y personas contratadas bajo cualquier modalidad de contratación que desempeñen funciones en otros organismos o entidades públicas no pertenecientes al Sector Público, por aplicación de lo dispuesto en un convenio de cooperación suscripto por el Certificador y dicho organismo o entidad.

Podrán también ser suscriptores de los certificados emitidos por la AC ONTI, los particulares que opten por realizar trámites electrónicos para los que el Sector Público requiera una firma digital.

Los certificados digitales emitidos por la AC ONTI podrán ser utilizados para firmar cualquier transacción electrónica asociada a la función correspondiente a cada suscriptor. Para el caso de los particulares, se podrán utilizar únicamente para la realización de trámites ante el Sector Público.

La Política correspondiente a la AC ONTI contempla y define dos niveles de seguridad para los certificados emitidos a favor de sus suscriptores:

- Nivel de seguridad Alto: para los certificados solicitados mediante el uso de dispositivos criptográficos (ej: tokens, smart cards).
- Nivel de seguridad Normal: correspondiente a los certificados solicitados y almacenados vía software.

El proceso de solicitud puede ser iniciado solamente por el interesado, quien posteriormente debe acreditar fehacientemente su identidad.

Al ingresar en el sitio web del certificador, debe seleccionar el enlace a la aplicación de solicitud de emisión de certificados para Personas Físicas del Sector Público y para particulares que realicen trámites ante el mismo, y completar los datos solicitados. Para el caso de funcionarios, agentes o personas contratadas en el Sector Público, se aceptará únicamente como dirección de correo electrónico válida, aquella que revista carácter institucional y se encuentre accesible por un cliente de correo electrónico.

Una vez ingresados sus datos y como paso previo a la generación del par de claves, seleccionará el nivel de seguridad del certificado requerido (alto o normal).

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos, de acuerdo con los niveles de seguridad establecidos previamente. En el caso que se utilicen dispositivos criptográficos, estos deberán ser homologados FIPS 140-2 Nivel 2. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

El par de claves del suscriptor de un certificado digital debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

La clave pública del solicitante es entregada a la aplicación de la AC ONTI durante el proceso de solicitud de certificado utilizando técnicas de “prueba de posesión” de la clave privada asociada

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la “prueba de posesión”, remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

APÉNDICE I – POLÍTICA DE CERTIFICACIÓN

Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado

Jefatura de Gabinete de Ministros

Secretaría de la Gestión Pública

Subsecretaría de Tecnologías de Gestión

Oficina Nacional de Tecnologías de Información

Versión 1.6

Septiembre, 2010

1. INTRODUCCIÓN

1.1. Descripción general

El presente documento define los términos que rigen la relación entre la Oficina Nacional de Tecnologías de Información (en adelante el Certificador) de la Subsecretaría de Tecnologías de Gestión de la Secretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros, las Autoridades de Registro (AR), los suscriptores y los terceros usuarios, en su condición de receptores de documentos firmados bajo la presente Política, en el marco del la Ley N° 25.506 de Firma Digital, su Decreto Reglamentario N° 2628/02 y la Decisión Administrativa Nº 6/07 y demás normas reglamentarias.

1.2. Identificación

Nombre: Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado

Versión: 1.0

Fecha de aplicación: 21 de Octubre de 2010

Sitio de publicación: http://pki.jgm.gov.ar/cps/cps.pdf

OID: 2.16.32.1.1.3

Lugar: Buenos Aires, Argentina

1.3. Participantes y aplicabilidad

Esta Política es aplicable a:

a) El Certificador, que emite certificados digitales para personas físicas

b) Las AR, que se constituyan en el ámbito de la presente Política

c) Los solicitantes y suscriptores de certificados digitales emitidos por el Certificador, en el ámbito de la presente Política

d) Los terceros usuarios, que verifican firmas digitales basadas en certificados digitales emitidos por el Certificador, en el ámbito de la presente Política.

1.3.1. Certificador

La Oficina Nacional de Tecnologías de Información (en adelante, la ONTI) en su calidad de Certificador, presta los servicios de certificación, de acuerdo con los términos de la presente Política.

1.3.2. Autoridad de Registro

El Certificador posee una estructura de AR que efectúan las funciones de validación de identidad y de otros datos de los solicitantes y suscriptores de certificados, registrando las presentaciones y trámites que les sean formulados por éstos.

Los entes públicos que han sido habilitados para operar como AR del Certificador se encuentran disponibles en su sitio web https://pki.jgm.gov.ar/app

Las AR serán autorizadas a funcionar como tales mediante notas firmadas por el del Director Nacional de la ONTI.

1.3.3. Suscriptores de certificados

Podrán ser suscriptores de los certificados emitidos por la Autoridad Certificante de la ONTI:

a) Las personas físicas que desempeñen funciones en entes públicos estatales o integren entes públicos no estatales.

b) Las personas físicas que realicen trámites con el Estado, cuando se requiera una firma digital.

En los casos de entes no pertenecientes a la Administración Pública Nacional, el Certificador podrá exigir previamente la suscripción de un acuerdo específico.

Además la AC ONTI será suscriptora de un certificado para ser usado en relación con el servicio On Line Certificate Status Protocol (en adelante, OCSP) de consulta sobre el estado de un certificado.

1.3.4. Aplicabilidad

Para el caso de personas físicas que desempeñen funciones en un ente público estatal, los certificados digitales emitidos en el marco de la presente Política podrán ser utilizados para firmar cualquier transacción electrónica asociada a la función correspondiente a cada suscriptor. En cualquier otro caso, solo se podrán utilizar para la realización de trámites ante el Estado.

La presente Política contempla también la emisión de certificados para responder a los requerimientos de verificación en línea del estado de los certificados (OCSP). Estos certificados, serán emitidos únicamente a favor de la AC ONTI.

La presente Política contempla y define dos niveles de seguridad para los certificados emitidos a favor de sus suscriptores (excluidos certificados OCSP):

a) Nivel de seguridad Alto: para los certificados solicitados mediante el uso de dispositivos criptográficos (ej: tokens, smart cards).

b) Nivel de seguridad Normal: correspondiente a los certificados solicitados y almacenados vía software.

1.4. Contactos

La presente Política de Certificación es administrada por:

Oficina Nacional de Tecnologías de Información

Domicilio: Roque Sáenz Peña 511 - 5° piso (C1035AAA) Ciudad Autónoma de Buenos Aires Argentina

Por consultas o sugerencias, dirigirse a:

Oficina Nacional de Tecnologías de Información

Domicilio: Roque Sáenz Peña 511 - 5° piso (C1035AAA) Ciudad Autónoma de Buenos Aires Argentina

Por correo electrónico: contactopki@sgp.gov.ar

Teléfono: (54 11) 4343-9001 Int. 519 / 521

Fax: (54 11) 4345-7458

2. ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACIÓN

2.1. Obligaciones

2.1.1. Obligaciones del certificador

De acuerdo a lo establecido en la Ley Nº 25.506, en su artículo 21:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;

q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

De acuerdo a lo establecido en el Decreto Nº 2628/02, en sus artículos 26, 32, 33 y 34:

Artículo 26:

a) Deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley N° 25.506, en el Decreto Nº 2628/02 y en las normas complementarias.

b) Someterse a auditorías anuales.

Artículo 32:

Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.

d) Expedir certificados que cumplan con:

1) Lo previsto en los artículos 13 y 14 de la Ley N° 25.506.

2) Los estándares tecnológicos aprobados por la Jefatura de Gabinete de Ministros.

e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.

f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.

g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.

h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.

i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.

j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.

k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.

l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Artículo 33:

Servicios de Terceros. En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción

de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Artículo 34:

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos. El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

r) El Certificador deberá cumplir además con toda otra obligación emanada de las prescripciones de la Decisión Administrativa Nº 6/07 y sus anexos complementarios y con aquellas establecidas en la presente Política de Certificación.

2.1.2. Obligaciones de la Autoridad de Registro

De acuerdo a lo establecido en el Decreto Nº 2628/02, en su artículo 35:

Una Autoridad de Registro es una entidad responsable de las siguientes funciones:

a) Recibir las solicitudes de emisión de certificados.

b) Validar la identidad y autenticación de los datos de los titulares de certificados.

c) Validar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador.

d) Remitir las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) Recibir y validar las solicitudes de revocación de certificados y su direccionamiento a la AC ONTI.

f) Identificar y autenticar los solicitantes de revocación de certificados.

g) Archivar y conservar toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) Cumplir las normas y recaudos establecidos para la protección de datos personales.

i) Cumplir las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador con el que se encuentre vinculada, en la parte que resulte aplicable.

De acuerdo a lo establecido en la Decisión Administrativa Nº 6/7, y con referencia a los Oficiales de Registro que desempeñen funciones en la AR:

Proteger su par de claves, de manera que su clave privada se encuentre en todo momento bajo su exclusivo conocimiento y control y con todas las medidas de seguridad establecidas por el certificador.

Adicionalmente para el caso de las AR que aprueben solicitudes de personas físicas que realicen trámites con el Estado y de aquellas que se constituyan en organismos o entidades no pertenecientes a la esfera nacional, deberán cumplir con lo dispuesto en el Acuerdo respectivo.

2.1.3. Obligaciones de los suscriptores del certificado

De acuerdo a lo establecido en la Ley Nº 25.506, en su artículo 25:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

c) Solicitar la revocación de su certificado al Certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

De acuerdo a lo establecido en la Decisión Administrativa Nº 06/07:

Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.

Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la presente Política de Certificación,

Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

2.1.4. Obligaciones de los terceros usuarios

De acuerdo a lo establecido en el punto 2.1.4 del Anexo II de la Decisión Administrativa N° 6/07:

a) Conocer los alcances de la Política de Certificación conforme a los Términos y condiciones con terceros usuarios;

b) Rechazar la utilización del certificado para aquellos fines distintos a los previstos en esta Política de Certificación;

c) Verificar la validez del certificado digital.

2.1.5. Obligaciones del servicio de repositorio

El Certificador está obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en el artículo 21 de la Ley N° 25.506, el Decreto N° 2628/02, y en la presente Política de Certificación.

Obligaciones establecidas en el artículo 21 inciso k) de la Ley N° 25.506:

a) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, la política de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la Autoridad de Aplicación.

Obligaciones establecidas en el artículo 34 incisos g), h) y m) del Decreto N° 2628/02:

a) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

b) Mantener actualizados los repositorios de certificados revocados por el período establecido por la Autoridad de Aplicación.

c) Cumplir con las normas y recaudos establecidos para la protección de datos personales.

Obligaciones adicionales y aclaraciones establecidas en la DA N° 6/07:

a) Disponer y dedicar los recursos establecidos para la seguridad de los datos almacenados, desde el punto de vista técnico y legal.

2.2. Responsabilidades

Conforme a lo dispuesto por la Ley N° 25.506, la relación entre el Certificador que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la citada ley, y demás legislación vigente. Esa relación conforme el artículo 37 de la mencionada ley quedará encuadrada dentro del ámbito de responsabilidad civil contractual.

Al emitir un certificado digital o al reconocerlo en los términos del artículo 16 de la Ley 25.506, el Certificador es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles todo ello de acuerdo con los establecido en el artículo 38 de la

Ley N° 25.506. Corresponderá al Certificador demostrar que actuó con la debida diligencia.

El artículo 36 del Decreto N° 2628/02, Reglamentario de la Ley N° 25.506, establece la responsabilidad del Certificador respecto de las AR.

En ese sentido prescribe que una AR puede constituirse como única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo delegar su operatoria en otras AR, siempre que medie la aprobación del Certificador.

El Certificador es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en AR, sin perjuicio del derecho del Certificador de reclamar a la AR las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

El Certificador tampoco es responsable en los siguientes casos, según el artículo 39 de la Ley antes mencionada:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados digitales y que no estén expresamente previstos en la Ley N° 25.506;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el Certificador pueda demostrar que ha tomado todas las medidas razonables.

Los alcances de la responsabilidad del Certificador se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en esta Política de Certificación en relación a la emisión, renovación y revocación de certificados. Los alcances de la responsabilidad del Certificador se limitan a los ámbitos de su incumbencia directa, en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los

certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.

El Certificador no garantiza el acceso a la información cuando mediaran razones de fuerza mayor (catástrofes naturales, cortes masivos de luz por períodos indeterminados, destrucción debido a eventos no previstos, etc.) ni asume responsabilidad por los daños o perjuicios que se deriven en forma directa o indirecta como consecuencia de estos casos.

2.3. Responsabilidad Financiera

2.3.1. Responsabilidad Financiera del Certificador

Las responsabilidades financieras se originan en lo establecido por la Ley 25.506 y su Decreto Reglamentario Nº 2628/02 y en las disposiciones de la presente Política.

2.4. Interpretación y aplicación de las normas

2.4.1. Legislación aplicable

La interpretación, obligatoriedad, diseño y validez de esta Política de Certificación se encuentran sometidos a lo establecido por la Ley Nº 25.506, su Decreto Reglamentario Nº 2628/02 y la Decisión Administrativa N° 06/07 y demás normas complementarias dictadas por la Autoridad de Aplicación.

2.4.2. Forma de interpretación y aplicación

La interpretación y/o aplicación de las disposiciones de la presente Política de Certificación y de cualquiera de sus documentos asociados, será resuelta según las normas mencionadas en el punto 2.4.1 y los procedimientos indicados en el punto 2.4.3.

Si se presentaren conflictos de interpretación de una o más disposiciones de esta Política de Certificación, el suscriptor o tercero usuario deberá agotar la vía administrativa con este Certificador, luego de cumplida esa instancia podrá accionar ante la Autoridad de Aplicación.

2.4.3. Procedimientos de resolución de conflictos

Cualquier controversia y/o conflicto resultante de la aplicación de esta Política de Certificación, deberá ser resuelta en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N° 1759/72.

La presente Política de Certificación se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506 y su reglamentación.

Los titulares de certificados y los terceros usuarios podrán efectuar reclamos ante el Ente Licenciante y eventualmente interponer recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por la AC ONTI, sólo será procedente previa acreditación de haberse efectuado reclamo ante el Certificador con resultado negativo. Acreditada dicha circunstancia, el Ente Licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción, de corresponder, del correspondiente trámite administrativo.

2.5. Aranceles

El Certificador no percibe aranceles por ninguno de los servicios que pudiera brindar relacionados con esta Política de Certificación. Los certificados emitidos bajo la presente Política son gratuitos y no se cobra ningún tipo de arancel o tasa por su solicitud, emisión, renovación, revocación o utilización.

2.6. Publicación y Repositorios de certificados y listas de certificados revocados (CRLs)

2.6.1. Publicación de información del certificador

El Certificador mantiene un repositorio en línea de acceso público que contiene:

a) Su certificado digital

b) Su certificado OCSP

c) La lista de certificados revocados (CRL)

d) La Política de Certificación en sus versiones vigente y anteriores

e) El Manual de Procedimientos en sus aspectos de carácter público, en sus versiones vigente y anteriores

f) El modelo del Acuerdo con Suscriptores

g) Los Términos y Condiciones con Terceros Usuarios

h) La Política de Privacidad

i) Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.

La información antedicha se encuentra disponible durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana en el sitio web del Certificador https://pki.jgm.gov.ar/app

2.6.2. Frecuencia de publicación

Producida una actualización de los documentos relacionados con el marco legal u operativo de la AC ONTI, estos documentos actualizados se publicarán dentro de las VEINTICUATRO (24) horas luego de ser aprobados por la Autoridad de Aplicación.

Asimismo, se emitirá cada VEINTICUATRO (24) horas la Lista de Certificados Revocados (CRL completa). Se emitirán CRL complementarias (delta CRL) con frecuencia horaria.

2.6.3. Controles de acceso a la información

El Certificador garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

2.6.4. Repositorios de certificados y listas de revocación

El servicio de repositorio de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por el Certificador.

El servicio de repositorio se encuentra disponible para uso público durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento.

2.7. Auditorías

El Certificador se encuentra sujeto a las auditorías de acuerdo a lo establecido en la Ley N° 25.506, su Decreto Reglamentario Nº 2628/02 y la Decisión Administrativa Nº 06/07.

La información relevante de los informes de las auditorías es publicada en el sitio web del certificador https://pki.jgm.gov.ar/app/ Se realiza una auditoría previa al licenciamiento del Certificador a fin de verificar el cumplimiento de los requisitos correspondientes al licenciamiento. Con posterioridad, el Certificador será sujeto a auditorías ordinarias para controlar la continuidad del cumplimiento de las normas vigentes y a auditorías extraordinarias de oficio, según lo disponga la Autoridad de Aplicación.

En su carácter de organismo comprendido en el artículo 8 de la Ley N° 24.156, el Certificador podrá ser auditado por la Sindicatura General de la Nación - SIGEN y por la Auditoría General de la Nación – AGN, en forma periódica.

Adicionalmente, el Certificador realizará auditorías periódicas sobre sus Autoridades de Registro.

2.8. Confidencialidad

2.8.1. Información confidencial

Toda información referida a solicitantes o suscriptores de certificados que sea recibida por el Certificador o por las AR operativamente vinculadas, será tratada en forma confidencial y no puede hacerse pública sin el consentimiento previo de los titulares de los datos, salvo que sea requerida judicialmente. La exigencia se extiende a toda otra información referida a los solicitantes y los suscriptores de certificados a la que tenga acceso el Certificador o sus AR durante el ciclo de vida del certificado.

Lo indicado no es aplicable cuando se trate de información que se transcriba en el certificado o sea obtenida de fuentes públicas.

El Certificador garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que

se especifique en la presente Política. Asimismo, se considera confidencial cualquier información:

Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por el Certificador Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa. Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.

En todos los casos resulta de aplicación la Ley N° 25.326 de protección de datos personales, su reglamentación y normas complementarias.

2.8.2. Información no confidencial

La siguiente información recibida por el Certificador o por sus AR no es considerada confidencial:

La que se encuentra contenida en su propio certificado digital La que se incluya en la CRL Toda otra referida a personas físicas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público.

Es considerada no confidencial la información incluida en los documentos publicados en el repositorio del Certificador mencionados en el apartado 2.6.1 de la presente Política..

2.8.3. Publicación de información sobre la revocación o suspensión de un certificado

La información contenida en la CRL referida a la revocación de un certificado no es considerada confidencial.

El servicio de repositorio se encuentra disponible para uso público durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento.

El estado de suspensión de un certificado no es aplicable en el marco de la Ley N° 25.506.

2.8.4. Divulgación de información a autoridades judiciales

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial.

2.8.5. Divulgación de información como parte de un proceso judicial o administrativo

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial o ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

2.8.6. Divulgación de información por solicitud del suscriptor

Toda divulgación de información referida a los datos de identificación del suscriptor o a cualquier otra información generada o recibida durante el ciclo de vida del certificado sólo podrá efectuarse previa autorización escrita del suscriptor del certificado.

No será necesario el consentimiento cuando:

Los datos se hayan obtenido de fuentes de acceso público irrestricto; Los datos se limiten a nombre, documento nacional de identidad, pasaporte, documento de identidad expedido por país miembro del MERCOSUR u ocupación. Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular

2.8.7. Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales el Certificador pueda divulgar la información.

2.9. Derechos de Propiedad Intelectual

El derecho de autor de los sistemas y aplicaciones informáticas desarrollados por el Certificador para la implementación de su AC, como así toda la documentación relacionada, pertenece a la ONTI.

El derecho de autor de la presente Política de Certificación y de toda otra documentación generada por el Certificador en relación con la Infraestructura de Firma Digital, pertenece a la ONTI. Consecuentemente, dichos documentos no pueden ser reproducidos, copiados ni utilizados de ninguna manera, total o parcial, sin previo y formal consentimiento de la ONTI, de acuerdo a la legislación vigente.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Registro inicial

El Certificador emite certificados a personas físicas, que cumplan con los requisitos para ser suscriptor, efectuándose una validación personal de la identidad del solicitante, para lo cual se requiere su presencia física ante el Oficial de Registro. Asimismo, el solicitante debe probar su carácter de suscriptor para esta Política de Certificación. La única excepción a la emisión de certificados para persona físicas es el caso del Certificado OCSP, mencionado precedentemente.

A fin de efectuar la validación de identidad indicada, el solicitante en forma personal, debe cumplir los siguientes pasos:

a) Ingresa al sitio web del Certificador https://pki.jgm.gov.ar/app/

b) Completa la solicitud de certificado con sus datos personales y selecciona el nivel de seguridad.

c) Acepta el Acuerdo con Suscriptores en el que se hace referencia a la Política que respalda la emisión del certificado.

d) Envía su solicitud a la AC ONTI e imprime la nota de solicitud.

e) Se presenta ante la AR correspondiente con la documentación requerida para realizar su identificación personal.

Cumplido el proceso de autenticación de su identidad, el solicitante firma la nota de solicitud de su certificado ante el Oficial de Registro de la AR correspondiente, con lo cual acepta las condiciones de emisión y uso del certificado.

3.1.1. Tipos de Nombres

Los Tipos de Nombres admitidos para los suscriptores de certificados son los que figuren en la documentación de identificación del solicitante.

3.1.2. Necesidad de Nombres Distintivos

Los atributos definidos a continuación son los mínimos incluidos en los certificados para identificar unívocamente a su titular, cualquiera sea su nivel de seguridad:

“commonName”: corresponde con los nombres y apellidos que figuran en el documento de identidad del solicitante o suscriptor.

“serialNumber”: contiene el tipo y número del documento del suscriptor. Se admitirán los siguientes documentos de identidad:

Para solicitantes que sean ciudadanos argentinos o residentes: Documento Nacional de Identidad, Libreta de Enrolamiento o Libreta Cívica. Para solicitantes extranjeros, Cédula de MERCOSUR, según las disposiciones vigentes, o Pasaporte y código de país emisor.

“title”: actividad, cargo o función del suscriptor dentro del ente público estatal. En el resto de los casos, actividad, pasividad, profesión u ocupación.

“emailAddress”: deberá contener la dirección de correo electrónico institucional del suscriptor, para el caso de entes públicos estatales. En el resto de los casos, salvo que posean una cuenta institucional, podrá ser definido en cada acuerdo a firmar con el Certificador.

“organizationalUnitName”: para el caso de las personas físicas de entes públicos estatales, contiene la información relativa al ente al que el suscriptor pertenece. Pueden existir varias ocurrencias de este atributo, representando la dependencia jerárquica del área del ente con la que se vincula el solicitante o suscriptor. En el resto de los casos, podrá ser definido en cada acuerdo a firmar con el Certificador.

“organizationName”: para el caso de personas físicas de entes públicos estatales, identifica la jurisdicción del Sector Público en la que desempeña sus funciones. Deberá consignar si pertenece al Sector Público, Provincial o Municipal, individualizando el Poder al que corresponde (Ejecutivo, Legislativo, Judicial o Ministerio Público) y la denominación de la Provincia o Municipio cuando sea aplicable. En el resto de los casos podrá ser definido en cada acuerdo a firmar con el Certificador.

“localityName”: identifica la localidad donde se desempeña el solicitante o suscriptor, en el caso de personas físicas de entes públicos, o la localidad donde reside, para las personas físicas que realicen trámites con el Estado.. En el caso de personas que residan en el exterior, se consignará la expresión “Provincia 25”.

“stateOrProvinceName”: identifica la provincia donde se desempeña el solicitante o suscriptor, en el caso de personas físicas de entes públicos, o la provincia donde reside, para las personas físicas que realicen trámites con el Estado.. En el caso de personas que residan en el exterior, se consignará la expresión “Provincia 25”.

“countryName”: debe contener el valor “AR”, por “Argentina” representando el país de emisión del certificador.

3.1.3. Reglas para la interpretación de nombres

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con los correspondientes al documento de identidad del suscriptor. Las discrepancias o conflictos que pudieran generarse cuando los datos de los solicitantes o suscriptores contengan caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

3.1.4. Unicidad de nombres

El nombre distintivo es único para cada suscriptor y está integrado por los campos indicados en el punto 3.1.2.

3.1.5. Procedimiento de resolución de disputas sobre nombres

El Certificador se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos que pudieran generarse respecto al uso y titularidad de nombres por parte de los solicitantes o suscriptores.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

No se aplica por tratarse de una Política de Certificación para personas físicas.

3.1.7. Métodos para comprobar la posesión de la clave privada

El solicitante o suscriptor generará su par de claves criptográficas usando su propio equipamiento durante el proceso de solicitud del certificado. Las claves son generadas y almacenadas por el solicitante, no quedando almacenada la clave privada en el sistema informático del Certificador.

En el caso de solicitudes de certificados de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo. Para certificados de nivel de seguridad Normal, el solicitante genera su par de claves y almacena la clave privada

vía software en su propio equipo al momento de la solicitud. La aplicación de la AC ONTI validará el requerimiento del certificado (PKCS#10) con el fin de verificar la posesión del la clave privada por parte del solicitante.

3.1.8. Autenticación de la identidad de personas jurídicas públicas o privadas

No se aplica por tratarse de una Política de Certificación para personas físicas.

3.1.9. Autenticación de la identidad de personas físicas

Según lo establecido en la presente Política de Certificación, el Certificador únicamente emite certificados para personas físicas que cumplan con los requisitos para ser suscriptor, efectuándose una validación de la identidad del solicitante, para lo cual se requiere su presencia física ante la AR correspondiente. Asimismo, el solicitante debe probar la titularidad de los datos contenidos en su solicitud.

La verificación se efectuará mediante la presentación de la siguiente documentación:

a) Documento Nacional de Identidad, Libreta Cívica o Libreta de Enrolamiento (original y fotocopia) para ciudadanos argentinos o residentes o Pasaporte o Cédula MERCOSUR (original y fotocopia) para extranjeros.

b) Para el caso de personas físicas de entes públicos estatales, Nota de certificación del cargo que ocupa. Esta podrá consistir en: Copia autenticada del Acto Administrativo correspondiente a su designación o Constancia emitida por la Oficina de Recursos Humanos, Personal o equivalente de su organismo o entidad, firmada por un funcionario responsable, en la que conste lugar y fecha de emisión, nombre y apellido, documento de identidad, organismo, unidad y cargo que ocupa en el mencionado organismo o entidad y los datos correspondientes al funcionario a quien reporta (Apellido y Nombre y cargo). Adicionalmente, deberá aumentarse una nota del funcionario de reporte del solicitante o suscriptor, indicando el cargo que éste ocupa.

c) Para el resto de los casos, podrá ser definido en cada acuerdo a firmar con el Certificador

d) Nota de solicitud de certificado, firmada por el solicitante.

El Oficial de Registro efectúa los siguientes pasos:

Verifica la existencia en el sistema de la solicitud, si correspondiese Al momento de presentación del solicitante o suscriptor en sus oficinas, valida su identidad mediante la verificación de la documentación requerida Verifica la titularidad de la solicitud mediante el control de la nota correspondiente, si fuera aplicable De corresponder, requiere al solicitante la firma de la nota de solicitud en su presencia Resguarda toda la documentación respaldatoria del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

El Certificador podrá autorizar un procedimiento en aquellos casos que exista un impedimento justificado que imposibilite la presentación física del solicitante o suscriptor ante la AR correspondiente, siempre que se garantice la identificación de su identidad.

3.2. Generación de nuevo par de claves (Re Key)

En caso de que por alguna causa resultase necesario cambiar el par de claves de un certificado vigente, el suscriptor deberá solicitar la revocación de su certificado e iniciar el proceso de solicitud de certificado. De haber expirado el certificado, no se permitirá la reutilización del mismo par de claves.

3.3. Generación de nuevo par de claves después de una revocación - Sin compromiso de claves

En caso de que por alguna causa resultase necesario cambiar el par de claves de un certificado vigente, el suscriptor deberá solicitar la revocación de su certificado e iniciar el proceso de solicitud de certificado. De haber expirado el certificado, no se permitirá la reutilización del mismo par de claves.

3.4. Requerimiento de revocación

Un suscriptor podrá revocar su certificado digital utilizando cualquiera de los siguientes métodos:

A través de la aplicación de la AC ONTI https://pki.jgm.gov.ar/app/ que se encuentra disponible VEINTICUATRO (24) horas, si tiene acceso a su clave privada.

A través de la aplicación de la AC ONTI https://pki.jgm.gov.ar/app/ que se encuentra disponible VEINTICUATRO (24) horas, utilizando el código de revocación que le fue entregado al momento de su solicitud.

En caso de no poder utilizar alguno de los anteriores, presentándose ante la AR correspondiente, con documento de identidad que permita acreditar su identidad.

En caso de suscriptores en entes públicos estatales, la revocación podrá ser solicitada por un funcionario competente del organismo indicado en el certificado, por nota dirigida al Responsable de la AR.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de certificado

4.1.1. Solicitud de nuevo certificado

Todo solicitante o suscriptor que se postule para obtener un certificado debe completar una solicitud, en el sitio web https://pki.jgm.gov.ar/app/ del Certificador, que estará sujeta a revisión y aprobación por la AR correspondiente.

El proceso de solicitud puede ser iniciado solamente por el interesado, quien posteriormente debe acreditar fehacientemente su identidad.

Al ingresar en el sitio web del certificador, debe seleccionar el enlace a la aplicación de solicitud de emisión de certificados para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado y completar los datos solicitados. Para el caso de funcionarios, agentes o personas contratadas en el Sector Público, se aceptará únicamente como dirección de correo electrónico válida aquella que revista carácter institucional y se encuentre accesible por un cliente de correo electrónico.

Una vez ingresados sus datos y como paso previo a la generación del par de claves, seleccionará el nivel de seguridad del certificado requerido (alto o normal).

Adicionalmente, el solicitante deberá leer y aceptar el Acuerdo con Suscriptores para continuar el proceso.

4.1.2. Solicitud de renovación

El proceso de renovación puede ser realizado solo si el certificado se encuentra vigente y debe ser iniciado solamente por el suscriptor, quien deberá tener acceso a su clave privada vinculada al certificado. Los datos contenidos en el certificado a renovar no deben haber variado. Caso contrario, deberá proceder a su revocación y posterior solicitud de un nuevo certificado, según lo dispuesto en el punto 4.1.1.

El suscriptor deberá ingresar al sitio web del Certificador https://pki.jgm.gov.ar/app/ y seleccionar la opción de renovación de certificados y seguir los pasos indicados.

La aprobación de la renovación está sujeta a la presentación de la documentación pertinente ante la AR que le corresponda.

4.2. Emisión del certificado

Cumplidos los recaudos del proceso de validación de identidad y otros datos del solicitante, de acuerdo con esta Política de Certificación y una vez aprobada la solicitud de certificado por la AR, la AC ONTI emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor.

4.3. Aceptación del certificado

Un certificado emitido por el Certificador se considera aceptado por su titular una vez que éste haya sido puesto a su disposición.

4.4. Suspensión y Revocación de Certificados

El estado de suspensión de certificados no es admitido en el marco de la Ley N° 25.506.

4.4.1. Causas de revocación

El Certificador revocará los certificados digitales que hubiera emitido en los siguientes casos:

A solicitud del titular del certificado Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros Por Resolución Judicial o Acto Administrativo de Autoridad competente

Por fallecimiento del titular Por declaración judicial de ausencia con presunción de fallecimiento del titular Por declaración judicial de incapacidad del titular Si se determina que la información contenida en el certificado ha dejado de ser válida Cuando la clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo. Cuando cese el vínculo entre el suscriptor y el ente o sea modificada su situación de revista o cargo Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores. Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital. Por revocación del certificado digital del Certificador Cuando así lo establezcan las condiciones indicadas en el Acuerdo aplicable a la AR, de existir

El Certificador, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

4.4.2. Autorizados a solicitar la revocación

Se encuentran autorizados a solicitar la revocación de un certificado emitido por el Certificador:

a) El suscriptor del certificado.

b) El máximo responsable del área de Recursos Humanos del ente público estatal en que se desempeñe el suscriptor del certificado.

c) La Autoridad competente del ente público de quien depende el suscriptor.

d) El Responsable del Certificador o de la AR correspondiente a ese suscriptor.

e) La Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina.

f) La Autoridad Judicial competente.

g) En el caso de certificados emitidos a favor de personas físicas no pertenecientes a entes públicos estatales, el Certificador procederá a la su revocación a solicitud de su titular o en los supuestos previstos en el acuerdo correspondiente.

4.4.3. Procedimientos para la solicitud de revocación

Para solicitar la revocación de su certificado, el suscriptor seguirá lo indicado en el apartado 3.4 Requerimiento de Revocación.

La AR conservará como documentación probatoria toda solicitud de revocación y el material probatorio vinculado.

Los suscriptores serán notificados en sus respectivas direcciones de correo electrónico o en la aplicación del Certificador, del cumplimiento del proceso de revocación.

4.4.4. Plazo para la solicitud de revocación

Las solicitudes de revocación se procesan en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.4.1.

El Certificador dispone de un servicio de recepción de solicitudes de revocación que se encuentra disponible en forma permanente, SIETE (7) x VEINTICUATRO (24) horas a través de la aplicación web de la AC ONTI.

El plazo máximo entre la de revocación y su publicación es de VEINTICUATRO (24) horas.

4.4.5. Causas de suspensión

El estado de suspensión no es admitido en el marco de la Ley N° 25.506.

4.4.6. Autorizados a solicitar la suspensión

No aplicable

4.4.7. Procedimientos para la solicitud de suspensión

No aplicable

4.4.8. Límites del periodo de suspensión de un certificado

No aplicable

4.4.9. Frecuencia de emisión de listas de certificados revocados

El Certificador genera y publica una Lista de Certificados Revocados con una frecuencia diaria con listas complementarias (delta CRL) en modo horario.

4.4.10. Requisitos para la verificación de la lista de certificados revocados

Los terceros usuarios están obligados a verificar el estado de validez de los certificados mediante el control de la lista de certificados revocados o en su defecto, mediante el servicio de consultas en línea sobre el estado de los certificados (OCSP), que el Certificador pondrá a su disposición.

Los terceros usuarios están obligados a confirmar la validez de la CRL mediante la verificación de la firma digital del Certificador y de su período de validez.

El Certificador garantiza el acceso permanente y gratuito del público en general a la CRL, disponible en su sitio web http://pki.jgm.gov.ar/crl/FD.crl

4.4.11. Disponibilidad en línea del servicio de revocación y verificación del estado del certificado

El Certificador posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento.

Ambos servicios se encuentran disponibles a partir de su sitio web https://pki.jgm.gov.ar/app

4.4.12. Requisitos para la verificación en línea del estado de revocación

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y representa una alternativa a la consulta a la CRL, la que también estará disponible. El servicio OCSP se provee por medio del sitio web http://pki.jgm.gov.ar/ocsp

4.4.13. Otras formas disponibles para la divulgación de la revocación

El Certificador no utiliza otros medios para la divulgación del estado de revocación de los certificados que los contemplados en la presente Política de Certificación.

4.4.14. Requisitos para la verificación de otras formas de divulgación de revocación

No aplicable

4.4.15. Requisitos específicos para casos de compromiso de claves

En caso de compromiso de la clave privada del suscriptor del certificado, éste es responsable de efectuar su revocación o bien de comunicar de inmediato tal situación al Responsable de la AR por algunas de las vías indicadas en el apartado 3.4 y el Certificador operará en consecuencia a lo establecido en la presente Política.

4.5. Procedimientos de Auditoría de Seguridad

El Certificador mantiene registros de auditoría de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros, que se conservarán por un plazo mínimo de DIEZ (10) años.

Asimismo, atendiendo a lo expresado en el punto 2.7 Auditoría, se mantendrán registros no informatizados de toda aquella información generada en formato de papel.

Estos registros se encuentran disponibles tanto para la auditoría interna como para la Autoridad de Aplicación y otros organismos o entidades que tengan competencias para acceder a esa información.

4.6. Archivo de registro de eventos

El Certificador mantiene un sistema de registro de archivos de transacciones que permite mantener en un entorno seguro toda la información considerada relevante y requerida, contemplando las siguientes actividades:

a) Administración del ciclo de vida de las claves criptográficas

b) Administración del ciclo de vida de los certificados

c) Información relacionada con la solicitud del certificado

d) Eventos de seguridad

Los archivos de registros se mantienen por un período de DIEZ (10) años a partir de su generación.

4.7. Cambio de claves criptográficas

El par de claves del Certificador ha sido generado con motivo del licenciamiento de la presente Política de Certificación y tendrá una vigencia de DIEZ (10) años. Por su parte la licencia tiene una vigencia de CINCO (5) años.

En todos los casos el cambio de claves criptográficas del certificador implica la emisión de un nuevo certificado por parte de la AC Raíz de la República Argentina. Si la clave privada del Certificador se encontrase comprometida, se procederá a la revocación de su certificado y esa clave ya no podrá ser usada en el proceso de emisión de certificados.

El Certificador tomará los recaudos necesarios para efectuar con suficiente antelación la renovación de su licencia y la obtención del certificado, si correspondiese.

4.8. Plan de contingencia y recuperación ante desastres

El Certificador ha implementado un Plan de contingencia ante hechos que comprometan la continuidad de sus operaciones, que garantiza el mantenimiento de sus servicios esenciales, los que incluirán como mínimo la recepción de solicitudes de revocación, y la consulta de CRL actualizadas y el servicio OSCP.

Dicho Plan de Contingencia describe los procedimientos que se implementan para minimizar las interrupciones de las actividades y para salvaguardar los procesos críticos, de las consecuencias de fallas significativas o masivas. El Plan involucra a la totalidad de los recursos físicos, software, personal e información, con el objeto de garantizar la adecuada y continua prestación de servicios.

Los procesos y procedimientos se encuentran definidos en dicho Plan, sobre el que se contemplan mecanismos de prueba y simulación con un periodicidad de SEIS (6) meses o cuando los cambios realizados sobre el hardware o software de base o aplicativo así lo ameriten.

4.9. Plan de Cese de Actividades

El Certificador cesará en su calidad de Licenciado de acuerdo con lo estipulado en el artículo 22 de la Ley N° 25506 por:

a) Decisión unilateral comunicada a la Autoridad de Aplicación

b) Disolución o reestructuración del organismo que ejerce las funciones de Certificador

c) Cancelación de su licencia dispuesta por la Autoridad de Aplicación, dados los supuestos previstos en el artículo 44 de la Ley 25.506

El Certificador dispone de un Plan de Cese de Actividades donde se contemplan las estrategias y procedimientos a seguir desde la declaración de cese hasta la inhabilitación lógica y física de sus instalaciones.

Declarado el cese, toda información del Certificador, cualquiera sea el soporte utilizado, será resguardada en el Archivo constituido a tal efecto,, por un plazo de DIEZ (10) años, incluyendo toda la documentación en poder de las AR. Si el cese se debiera a la disolución o reestructuración del organismo, los registros serán transferidos al organismo al que se le asignen las funciones correspondientes.

5. CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

La descripción detallada de los procedimientos referidos a los controles de seguridad física, funcional y del personal se desarrolla en el Plan de Seguridad del Certificador.

5.1. Controles de seguridad física

El Certificador implementa controles apropiados que restringen el acceso a los equipos, programas y datos utilizados para proveer el servicio de certificación, solamente a personas debidamente autorizadas.

Se implementan procedimientos de control sobre los siguientes aspectos:

a) Construcción y localización de instalaciones

b) Acceso físico

c) Energía y aire acondicionado

d) Exposición al agua

e) Prevención y protección contra incendios

f) Medios de almacenamiento

g) Disposición de material de descarte

h) Instalaciones de seguridad externas

5.2. Controles Funcionales

Las funciones del Certificador son llevadas a cabo por personal calificado y son realizadas de acuerdo a roles asignados a tal efecto, descriptos en el Documento “Roles y Funciones” del Certificador.

La autoridad competente del organismo o quien éste designe, asignará dichos roles, respetando los siguientes criterios:

a) Cada uno de los roles tiene un titular asignado y por lo menos, un sustituto

b) Se asegurará una adecuada separación de funciones, a fin de evitar incompatibilidades en la asignación de los roles mencionados

En el caso de las AR, el Certificador efectuará los controles funcionales pertinentes, verificando el cumplimiento de las responsabilidades y procedimientos según lo dispuesto en la presente Política de Certificación y demás documentación del Certificador.

Las personas que ejercen cada uno de los roles mencionados dispondrán de adecuadas credenciales de identificación y autenticación, cuando fuera aplicable, de acuerdo a las tareas que desempeñen.

5.3. Controles de Seguridad del Personal

El Certificador sigue una política de administración de personal que provee razonable seguridad acerca de la confiabilidad y competencia del personal para el adecuado cumplimiento de sus funciones.

Se establecen procedimientos de control sobre los siguientes aspectos:

a) Antecedentes penales, laborales, de competencia e idoneidad conforme los requisitos establecidos para la contratación o designación en los regímenes aplicables.

b) Instancias de capacitación vinculadas a los roles y tareas que se desempeñan, con la frecuencia de actualización técnica requerida en cada caso.

c) Sanciones a aplicar de acuerdo a los regímenes de contratación o designación aplicables, según corresponda

d) Credenciales, elementos de identificación personal y demás documentación provista al personal que desempeñe funciones en el Certificador.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación de claves

6.1.1. Generación del par de claves criptográficas

El Certificador, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política, generará el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits.

En el caso de las AR, cada Oficial de Registro generará y almacenará su par de claves utilizando un dispositivo criptográfico homologado FIPS 140-2 Nivel 2 y utilizando el algoritmo RSA con un tamaño mínimo de 1024 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos, de acuerdo con los niveles de seguridad establecidos en el punto 1.3.1. En el caso que se utilicen dispositivos criptográficos, estos deberán ser homologados FIPS 140-2 Nivel 2. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

El par de claves del suscriptor de un certificado emitido en los términos de esta Política de Certificación debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

6.1.2. Entrega de la clave privada al suscriptor

El Certificador se abstendrá de generar, exigir o por cualquier medio tomar conocimiento o acceder a la clave privada de los suscriptores, de acuerdo a lo dispuesto por la Ley 25.506 artículo 21 inc. b) y el Decreto Nº 2628/02 artículo 34 inc. i).

6.1.3. Entrega de la clave pública al emisor del certificado

El solicitante entregará su clave pública a la AC ONTI, a través de la aplicación correspondiente, durante el proceso de solicitud de su certificado. La AC ONTI por su parte utilizará técnicas de "prueba de posesión" para determinar que el solicitantes se encuentra en posesión de la clave privada asociada a dicha clave pública.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión", remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

El procedimiento descripto asegura que:

La clave pública no pueda ser cambiada durante la transferencia. Los datos recibidos por el Certificador se encuentran vinculados a dicha clave pública El remitente posee la clave privada que corresponde a la clave pública transferida.

6.1.4. Disponibilidad de la clave pública del Certificador

El certificado del Certificador y su cadena de certificación se encuentran a disposición de los suscriptores y terceros usuarios en un repositorio en línea de acceso público a través de Internet, accesible a partir de https://pki.jgm.gov.ar/app/

6.1.5. Tamaño de claves

La longitud de las claves criptográficas del certificado del Certificador es de 4096 bits.

La longitud de las claves criptográficas de los certificados de suscriptores emitidos por el Certificador es de 1024 bits como mínimo.

El algoritmo de firma utilizado es SHA-1 con RSA.

6.1.6. Generación de parámetros de claves asimétricas

No se establecen condiciones especiales para la generación de parámetros de claves asimétricas más allá de las que se indican en el punto 6.1.5.

6.1.7. Verificación de calidad de los parámetros

La verificación de calidad de los parámetros será realizada por la aplicación del Certificador. Esta verificación abarca la correcta longitud de la clave y la utilización de los algoritmos especificados en esta sección.

6.1.8. Generación de claves por hardware o software

Para la generación de claves criptográficas, el Certificador utiliza dispositivos de las siguientes características:

Para la generación de las claves criptográficas del Certificador: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 3.

Para la generación de las claves criptográficas utilizadas para la firma de información de estado de certificados: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 3.

Para la generación de las claves criptográficas utilizadas por las AR para la aprobación de solicitudes, de renovaciones o revocaciones: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 2.

Para certificados de suscriptores de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo criptográfico especial que cumple con las características definidas en FIPS 140-2 para el nivel 2.

Para certificados de nivel de seguridad Normal, el solicitante genera su par de claves y almacena la clave privada vía software al momento de la solicitud.

6.1.9. Propósitos de utilización de claves (campo “Key Usage” en certificados X.509 v.3)

Las claves contenidas en los certificados emitidos por la AC ONTI tienen como propósito su utilización para firmar digitalmente, por lo que los valores a utilizar en la extensión “KeyUsage” de los certificados son Firma Digital (“digitalSignature”) y No Repudio (“nonRepudiation”).

6.2. Protección de la clave privada

6.2.1. Estándares para dispositivos criptográficos

Para la generación y el almacenamiento de las claves criptográficas, el Certificador, las AR y los suscriptores que opten por un nivel Alto para sus certificados, utilizan los dispositivos referidos en el apartado 6.1.1.

6.2.2. Control “M de N” de clave privada

El procedimiento de utilización de las claves privadas del Certificador se efectúa en forma segura, de manera tal que siempre es necesaria la presencia de una cantidad determinada de personas distintas para su activación de un universo mayor posible.

6.2.3. Recuperación de clave privada

Ante una situación que requiera recuperar su clave privada, y siempre que ésta no se encuentre comprometida, el Certificador cuenta con procedimientos para su recuperación. Esta sólo puede ser realizada por personal autorizado, sobre dispositivos criptográficos seguros y exclusivamente en el nivel de seguridad donde se realicen las operaciones críticas de la AC ONTI.

No se implementan mecanismos de resguardo y recuperación de las claves privadas de las AR y de los suscriptores. Estos deberán proceder a la revocación del certificado y a tramitar una nueva solicitud de emisión de certificado, si así correspondiere.

6.2.4. Copia de seguridad de la clave privada

El Certificador genera una copia de seguridad de la clave privada a través de un procedimiento que garantiza su integridad y confidencialidad.

No se mantienen copias de las claves privadas de los suscriptores de certificados ni de los Oficiales de Registro.

6.2.5. Archivo de clave privada

El Certificador almacena las copias de reguardo de su clave privada a través de un procedimiento que garantiza su integridad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación, de acuerdo a lo dispuesto por la Decisión Administrativa Nº 06/07 en cuanto a los niveles de reguardo de claves.

6.2.6. Incorporación de claves privadas en dispositivos criptográficos

El par de claves criptográficas del Certificador se genera y almacena en dispositivos criptográficos conforme a lo establecido en la presente Política, salvo en el caso de las

copias de resguardo que también están soportados en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

El par de claves criptográficas de las AR y de los suscriptores de certificados de nivel de seguridad Alto es almacenado en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se genera, no permitiendo su exportación.

6.2.7. Método de activación de claves privadas

Para la activación de la clave privada de la AC ONTI se aplican procedimientos que requieren la participación de los poseedores de claves de activación según el control M de N descripto más arriba, quienes validan las operaciones críticas, autorizando su ejecución por medio de llaves especiales que obran en su poder.

6.2.8. Método de desactivación de claves privadas

La desactivación de las claves privadas se lleva adelante mediante el proceso de desactivación de partición; cuando se requiere utilizar temporalmente un equipamiento de respaldo o se realicen tareas de mantenimiento.

6.2.9. Método de destrucción de claves privadas

Las claves privadas se destruyen mediante procedimientos que imposibilitan su posterior recuperación o uso, bajo las mismas medidas de seguridad que se emplearon para su creación.

6.3. Otros aspectos de administración de claves

6.3.1. Archivo Permanente de clave pública

Los certificados emitidos a suscriptores y a los Oficiales de Registro como así también el de la AC ONTI son almacenados bajo un esquema de redundancia y respaldados en forma periódica sobre dispositivos de solo lectura, lo cual sumado a la firma de los mismos, garantiza su integridad.

Los certificados se almacenan en formato estándar bajo codificación internacional DER.

6.3.2. Período de uso de clave pública y privada

La clave privada asociada con el certificado digital del Certificador, tiene una validez de DIEZ (10) años.

Los certificados digitales de las AR y de los suscriptores tendrán una validez de DOS (2) años.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación del dispositivo criptográfico del certificador tienen un control "M de N" en base a "M" Poseedores de claves de activación, que deben estar presentes de un total de "N" Poseedores posibles.

Ni el Certificador ni las AR implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores u Oficiales de Registro o a sus dispositivos criptográficos, si fuera aplicable.

6.4.2. Protección de los datos de activación

El Certificador establece medidas de seguridad para proteger adecuadamente los datos de activación de su clave privada contra usos no autorizados. En este sentido, instruirá a los poseedores de las claves de activación para el uso seguro y resguardo de los dispositivos correspondientes.

6.4.3. Otros aspectos referidos a los datos de activación

Es responsabilidad de los Oficiales de Registro y de los suscriptores de certificados emitidos por la AC ONTI, elegir contraseñas fuertes para la protección de sus claves privadas y para el acceso a los dispositivos criptográficos que utilicen, si fuera aplicable.

6.5. Controles de seguridad Informática

6.5.1. Requisitos Técnicos específicos

El Certificador establece los controles de seguridad referidos a su equipamiento que cumple con los requisitos técnicos definidos por la normativa vigente.

Los controles implementados se refieren a los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación

b) El Certificador implementa controles de seguridad físicos y lógicos para proteger por una lado el acceso a las instalaciones de la AC ONTI y por otro, el acceso lógico a los sistemas involucrados en la gestión del Certificador

c) Separación de funciones para los roles de certificación

d) Existe una adecuada separación de funciones, no asignándose funciones o roles incompatibles a los intervinientes.

e) Identificación y autenticación de los roles afectados al proceso de certificación

f) Se gestionará una autenticación robusta (2 factores como mínimo) para todos los roles afectados al proceso de certificación.

g) Utilización de criptografía para las sesiones de comunicación y bases de datos

h) Las comunicaciones entre los componentes críticos de la AC ONTI se realizan en forma cifrada.

i) Archivo de datos históricos y de auditoría del Certificador y usuarios

j) Se almacenarán y archivarán los datos históricos y de auditoría del Certificador como así también los correspondientes a los trámites de los suscriptores.

k) Registro de eventos de seguridad

l) Todas las operaciones y actividades de la AC ONTI ocurridas durante el proceso de certificación generan información de control y registros de eventos que permiten verificar el correcto funcionamiento y la seguridad de los sistemas.

m) Prueba de seguridad relativa a servicios de certificación

n) Se realizarán pruebas periódicas de seguridad de los servicios involucrados en los procesos de certificación.

o) Mecanismos confiables para identificación de roles afectados al proceso de certificación

p) Los sistemas y servicios que gestionan las tareas de certificación, poseen mecanismos confiables para identificación de roles.

q) Mecanismos de recuperación para claves y sistema de certificación

r) En el documento Plan de Contingencia se describen los mecanismos de recuperación de los sistemas para garantizar la continuidad de operaciones.

Las funcionalidades mencionadas son provistas a través de una combinación del sistema operativo, software aplicativo y controles físicos.

La descripción de los controles de seguridad establecidos sobre los servidores del Certificador se incluye en el Plan de Seguridad.

6.5.2. Calificaciones de seguridad computacional

El certificador cumple con las siguientes calificaciones de seguridad sobre los productos en los que se basa la implementación:

Windows 2008 R2 Server Enterprise: en proceso de evaluación para certificar EAL4+ Windows 2008 Server Enterprise x86: certificado EAL4+ Forefront TMG 2010 Enterprise x64: en proceso de evaluación para certificar EAL4+ SQL 2008 Enterprise x64 SP1: certificado EAL4+ Forefront Client Security:-Sin certificar System Center Data Protection Manager 2010:- Sin certificar

6.6. Controles Técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

El Certificador cumple con procedimientos específicos para el diseño y desarrollo de sistemas entre los que se encuentran:

a) Separación de ambientes de desarrollo, prueba y producción

b) Control de versiones para los componentes desarrollados

6.6.2. Controles de administración de seguridad

Existen controles respecto a la integridad del sistema de archivos de la AC ONTI que permiten controlar si hubo alteraciones no autorizadas.

6.6.3. Calificaciones de seguridad del ciclo de vida

No aplicable

6.7. Controles de seguridad de red

Los servicios que provee el Certificador que se encuentran conectados a una red de comunicación pública, son protegidos por la tecnología apropiada que garantiza su seguridad.

6.8. Controles de ingeniería de módulos criptográficos

El dispositivo criptográfico utilizado por el certificador está certificado por el NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por las AR están certificados por NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

Los dispositivos criptográficos utilizados por suscriptores de nivel de seguridad Alto están certificados por NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

7. Perfiles de Certificados y de Listas de Certificados Revocados

7.1. Perfil del certificado

Los certificados emitidos por el Certificador respaldados por esta Política de Certificación cumplen con los requerimientos de la DA 6/2007 y lo establecido en la especificación ITU X509 versión 3 (ISO/IEC 9594-8), adoptada como Estándar Técnico de la Infraestructura de Firma Digital de la República Argentina.

El Certificador adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” [RFC3739]. RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC5280].

7.1.1. Perfil del certificado de la persona física

Certificado x.509 v3 Nombre del campo y OID Contenido Atributos Extensiones

Versión (Version)

V3 2 (correspondiente a versión 3)

Número de serie (SerialNumber)

Serial Number 2.5.4.5

<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)

Algoritmo de Firma (SignatureAlgoritm)

1.2.840.113549.1.1.5

sha1RSA

Nombre distintivo del emisor (Issuer)

commonName - 2.5.4.3

CN=Autoridad Certificante de Firma Digital

serialNumber - 2.5.4.5

SERIALNUMBER=CUIT 30680604572

organizationName - 2.5.4.10

O=Jefatura de Gabinete de Ministros

organizationalUnitName - 2.5.4.11

OU=Oficina Nacional de Tecnologías de Información

stateOrProvinceName - 2.5.4.8

S=Ciudad Autónoma de Buenos Aires

countryName - 2.5.4.6

C=AR

Validez (desde, hasta)

notBefore

<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario

(notBefore/notAfter)

notAfter

<fecha y hora de emisión UTC+ 2 años> yyyy/mm/dd hh:mm:ss huso-horario

Nombre distintivo del suscriptor (Subject DN)

commonName - 2.5.4.3

CN=APELLIDO Nombre

email

E=<dirección de correo del suscriptor>

serialNumber - 2.5.4.5

SERIALNUMBER=<Tipo> <Número de documento> <Versión=1 char>

title - 2.5.4.12

T=<Nombre del cargo> o <lo indicado en el convenio correspondiente> (posición o función del suscriptor dentro de la organización, debe corresponder con los atributos O/OU y con la certificación de cargo presentada)

organizationName - 2.5.4.10

O=<Nombre de la organización> o <lo indicado en el convenio correspondiente>

organizationalUnitName - 2.5.4.11

OU=<Nombre de la unidad donde desarrolla su función> o <lo indicado en el convenio correspondiente>

localityName - 2.5.4.7

L=<Nombre de localidad>

stateOrProvinceName - 2.5.4.8

S = <Nombre de la provincia>

countryName - 2.5.4.6

C=AR

Clave pública del suscriptor

public key algorithm 1.2.840.11.35.49.1.1.1

RSA

Public key length

1024 bits

Clave pública del suscriptor

<Clave pública del suscriptor>

Restricciones básicas (Basic Constraints)

basicConstraint 2.5.29.19

Tipo de asunto = Entidad final pathLenghtConstraint = Null

Usos de clave (Key Usage)

keyUsage 2.5.29.15

digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0

Identificador de clave del asunto (Subject Key Identifier)

(Subject Key Identifier)

Contiene un hash de 20 bytes del atributo clave pública del suscriptor

Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)

CRLDistributionPoints - 2.5.29.31

[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl

Bases del certificado

[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://pki.jgm.gov.ar/cps/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: http://pkicont.jgm.gov.ar/cps/cps.pdf Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la República Argentina, Autoridad Certificante Raíz

Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)

AuthorityKeyIdentifier 2.5.29.35

keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.)

Uso Extendido de Clave (Extended Key Usage)

ExtendedKeyUsage 2.5.29.37

Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)

Nombres Alternativos del Suscriptor (Subject Alternative Name)

SubjectAltName 2.5.29.17

Name = <Dirección de correo electrónico> (dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822)

Acceso Información Emisor (Authority Information Access)

[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pki.jgm.gov.ar/aia/cafdONTI.crt [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pkicont.jgm.gov.ar/aia/cafdONTI.crt [3]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pki.jgm.gov.ar/ocsp [4]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pkicont.jgm.gov.ar/ocsp Nombre alternativo: Dirección URL=http://PKI.jgm.gov.ar/ocsp Dirección URL=http://PKIcont.jgm.gov.ar/ocsp

Algoritmo de Identificación

SHA1

Huella Digital

<Huella digital del certificado>

Información de la plantilla de certificado

Plantilla=1.3.6.1.4.1.311.21.8.15857867.913644.13845672.12138563.12347226.69.335 1984.12088013 Número de versión mayor=100 Número de versión menor=2

Directivas de aplicación

[1]Directiva de certificado de la aplicación: Identificador de directiva=Autenticación del cliente [2]Directiva de certificado de la aplicación: Identificador de directiva=Correo seguro

Certificado x.509 v3 Nombre del campo y OID Contenido Atributos Extensiones

Versión (Version)

V3 2 (correspondiente a versión 3)

Número de serie (SerialNumber)

Serial Number 2.5.4.5

<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)

Algoritmo de Firma (SignatureAlgoritm)

1.2.840.113549.1.1.5

sha1RSA

Nombre distintivo del emisor (Issuer)

commonName - 2.5.4.3

CN=Autoridad Certificante de Firma Digital

serialNumber - 2.5.4.5

SERIALNUMBER=CUIT 30680604572

organizationName - 2.5.4.10

O=Jefatura de Gabinete de Ministros

organizationalUnitName - 2.5.4.11

OU=Oficina Nacional de Tecnologías de Información

stateOrProvinceName - 2.5.4.8

S=Ciudad Autónoma de Buenos Aires

countryName - 2.5.4.6

C=AR

Validez (desde, hasta)

notBefore

<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario

(notBefore/notAfter)

notAfter

<fecha y hora de emisión UTC+ 2 años> yyyy/mm/dd hh:mm:ss huso-horario

Nombre distintivo del suscriptor (Subject DN)

commonName - 2.5.4.3

CN=APELLIDO Nombre

email

E=<dirección de correo del suscriptor>

serialNumber - 2.5.4.5

SERIALNUMBER=<Tipo> <Número de documento> <Versión=1 char>

title - 2.5.4.12

T=<Nombre del cargo> o <lo indicado en el convenio correspondiente> (posición o función del suscriptor dentro de la organización, debe corresponder con los atributos O/OU y con la certificación de cargo presentada)

organizationName - 2.5.4.10

O=<Nombre de la organización> o <lo indicado en el convenio correspondiente>

organizationalUnitName - 2.5.4.11

OU=<Nombre de la unidad donde desarrolla su función> o <lo indicado en el convenio correspondiente>

localityName - 2.5.4.7

L=<Nombre de localidad>

stateOrProvinceName - 2.5.4.8

S = <Nombre de la provincia>

countryName - 2.5.4.6

C=AR

Clave pública del suscriptor

public key algorithm 1.2.840.11.35.49.1.1.1

RSA

Public key length

2048 bits

Clave pública del suscriptor

<Clave pública del suscriptor>

Restricciones básicas (Basic Constraints)

basicConstraint 2.5.29.19

Tipo de asunto = Entidad final pathLenghtConstraint = Null

Usos de clave (Key Usage)

keyUsage 2.5.29.15

digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0

Identificador de clave del asunto (Subject Key Identifier)

(Subject Key Identifier)

Contiene un hash de 20 bytes del atributo clave pública del suscriptor

Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)

CRLDistributionPoints - 2.5.29.31

[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl

Bases del certificado

[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://pki.jgm.gov.ar/cps/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: http://pkicont.jgm.gov.ar/cps/cps.pdf Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la República Argentina, Autoridad Certificante Raíz

Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)

AuthorityKeyIdentifier 2.5.29.35

keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.)

Uso Extendido de Clave (Extended Key Usage)

ExtendedKeyUsage 2.5.29.37

Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)

Nombres Alternativos del Suscriptor (Subject Alternative Name)

SubjectAltName 2.5.29.17

Name = <Dirección de correo electrónico> (dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822)

Acceso Información Emisor (Authority Information Access)

[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pki.jgm.gov.ar/aia/cafdONTI.crt [2]Acceso a información de autoridad

Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pkicont.jgm.gov.ar/aia/cafdONTI.crt [3]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pki.jgm.gov.ar/ocsp [4]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pkicont.jgm.gov.ar/ocsp Nombre alternativo: Dirección URL=http://PKI.jgm.gov.ar/ocsp Dirección URL=http://PKIcont.jgm.gov.ar/ocsp

Algoritmo de Identificación

SHA1

Huella Digital

<Huella digital del certificado>

Información de la plantilla de certificado

Plantilla=1.3.6.1.4.1.311.21.8.15857867.913644.13845672.12138563.12347226.69.335 1984.12088013 Número de versión mayor=100 Número de versión menor=2

Directivas de aplicación

[1]Directiva de certificado de la aplicación: Identificador de directiva=Autenticación del cliente [2]Directiva de certificado de la aplicación: Identificador de directiva=Correo seguro

7.1.2. Perfil del certificado del servicio de consulta OCSP

En lo referente a OCSPs el certificador adhiere a las recomendaciones del documento:

Certificado x.509 v3 OIDs Contenido Atributos Extensiones Versión (Version) 2 (correspondiente a versión 3) Número de serie (SerialNumber) Serial Number 2.5.4.5 <Número de serie del certificado> Algoritmo de Firma (SignatureAlgorithm) 1.2.840.113549.1.1.5 sha1RSA Nombre distintivo del emisor (Issuer) commonName - 2.5.4.3 CN=Autoridad Certificante de Firma Digital serialNumber - 2.5.4.5 SERIALNUMBER=CUIT 30680604572 organizationName - 2.5.4.10 O=Jefatura de Gabinete de Ministros, Secretaría de la Gestión Pública, Subsecretaría de Tecnologías de Gestión organizationalUnitName - 2.5.4.11 OU=Oficina Nacional de Tecnologías de

Información stateOrProvinceName - 2.5.4.8 S=Ciudad Autónoma de Buenos Aires countryName - 2.5.4.6 C=AR Validez (desde, hasta) notBefore <fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario notAfter <fecha y hora de emisión UTC+ 7 dias> yyyy/mm/dd hh:mm:ss huso-horario

Nombre distintivo del suscriptor (Subject) commonName - 2.5.4.3 CN = PKIWEBSW001V.ACPKI.AR commonName = Servicio OCSP Clave pública del suscriptor (Subject public key info) public key algorithm 1.2.840.11.35.49.1.1.1 RSA Public key length 1024 bits Clave pública del suscriptor <Clave pública del suscriptor> (PKCS#1) Restricciones básicas (Basic Constraints) basicConstraint 2.5.29.19 cA = False pathLengthConstraint = Null Usos de clave (Key Usage) keyUsage 2.5.29.15 digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0 Identificador de clave del asunto (Subject Key Identifier) b6 a6 56 b4 6f 04 7f 88 60 8f f8 4c 48 31 45 d9 0c 70 d2 0c Contiene un Hash de 20 bytes del atributo clave pública del suscriptor Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) CRLDistributionPoints 2.5.29.31 [1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl Bases del certificado [1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://pki.jgm.gov.ar/cps/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: http://pkicont.jgm.gov.ar/cps/cps.pdf Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la Republica Argentina, Autoridad Certificante Raiz Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier) AuthorityKeyIdentifier 2.5.29.35 Id. de clave=70 ba 03 71 7a d8 10 e4 ee 52 b5 7f 32 8f 9f 6c 2e f7 84 0d keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.)

Uso Extendido de Clave (Extended Key Usage) Firma de OCSP (1.3.6.1.5.5.7.3.9) OCSP signing id-kp-OCSPSigning oid 1.3.6.1.5.5.7.3.9 Nombres Alternativos del Suscriptor (Subject Alternative Name) SubjectAltName 2.5.29.17 Nombre

DNS=PKIWEBSW001V.ACPKI.AR Acceso Información Emisor (Authority Information Access) caIssuers <http> <URL> [1]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.jgm.gov.ar/pki/cer/ONTIAC.cer caOCSP <http> <URL> [2]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://www.jgm.gov.ar/pki/ocsp/ Algoritmo de Identificación SHA1 Huella Digital <Huella digital de la CRL> Información de la plantilla de certificado Plantilla=1.3.6.1.4.1.311.21.8.15857867.913644.13845672.12138563.12347226.69.3520907.9008002 Número de versión mayor=100 Número de versión menor=1 Directivas de aplicación [1]Directiva de certificado de la aplicación: Identificador de directiva=Firma de OCSP Comprobacion de no revocacion de OCSP 05 00

7.1.3. Perfil del certificado de AC

Certificado x.509 v3 OIDs Contenido Atributos Extensiones

Versión (Version)

V3 2 (correspondiente a versión 3)

Número de serie (SerialNumber)

Serial Number 2.5.4.5

<Número de serie del certificado> (entero positivo asignado unívocamente por la CA RAIZ a cada certificado de hasta 20 octetos)

Algoritmo de Firma (SignatureAlgoritm)

1.2.840.113549.1.1.5

sha1RSA 1.2.840.113549.1.1.5 SHA 1 with RSA Encryption

Nombre distintivo del emisor

commonName - 2.5.4.3

CN =AC Raíz

serialNumber - 2.5.4.5

SERIALNUMBER=

organizationName - 2.5.4.10

O = Infraestructura de Firma Digital

countryName - 2.5.4.6

C = AR

Validez (desde, hasta)

notBefore

<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario

(notBefore/notAfter)

notAfter

<fecha y hora de emisión UTC+ 10 años> yyyy/mm/dd hh:mm:ss huso-horario

Nombre distintivo del suscriptor (Subject DN)

commonName - 2.5.4.3

CN=Autoridad Certificante de Firma Digital

serialNumber - 2.5.4.5

SERIALNUMBER=CUIT 30680604572

organizationName - 2.5.4.10

O=Jefatura de Gabinete de Ministros

organizationalUnitName - 2.5.4.11

OU=Oficina Nacional de Tecnologías de Información

OU=Secretatria de Gestion Publica

OU= Subsecretaria de Tecnologias de Gestion

stateOrProvinceName - 2.5.4.8

S=Ciudad Autónoma de Buenos Aires

countryName - 2.5.4.6

C=AR

Clave pública del suscriptor (Subject public key info)

Public Key Algorithm

RSA

Publick key leght

4096 bits

Clave pública del suscriptor

<Clave pública del suscriptor>

Restricciones básicas (Basic Constraints)

Tipo de asunto=Entidad emisora de certificados (CA) Restricción de longitud de ruta=0 CA = TRUE PathRestriccionLength= 0

Usos de clave (Key Usage)

digitalSignature = 0 nonRepudiation = 0 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 1 cRLSign = 1 encipherOnly = 0 decipherOnly = 0

Identificador de clave del asunto (Subject Key Identifier)

Contiene un Hash de 20 bytes del atributo clave pública del suscriptor

Puntos de Distribución de la Lista de Certificados Revocados (CRL Distribution Point)

DistributionPoint [1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://acraiz.cdp1.gov.ar/ca.crl [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://acraiz.cdp2.gov.ar/ca.crl

Bases del Certificado

[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://acraiz.gov.ar/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la Republica Argentina, Autoridad Certificante Raiz

Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)

keyIdentifier = <Identificador de la clave de la AC>

Acceso Información Emisor (Authority Information Access)

[1]Acceso a información de Emisor Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://acraiz.gov.ar/ca.crt

Algoritmo de Identificación

SHA1

Huella Digital

<xx xx>

7.2. Perfil de la lista de certificados revocados

En lo referente a CRLs el certificador adhiere a las recomendaciones del documento:

RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC5280]

Atributos Extensiones Nombre del campo y OID Contenido

Versión (Version)

1 (correspondiente a versión 2)

Algoritmo de Firma (SignatureAlgorithm)

1.2.840.113549.1.1.5

SHA1RSA

Nombre distintivo del emisor (Issuer)

commonName - 2.5.4.3

CN=Autoridad Certificante de Firma Digital

serialNumber - 2.5.4.5

SERIALNUMBER=CUIT 30680604572

organizationName - 2.5.4.10

O=Jefatura de Gabinete de Ministros, Secretaría de la Gestión Pública, Subsecretaría de Tecnologías de Gestión

organizationalUnitName - 2.5.4.11

OU=Oficina Nacional de Tecnologías de Información

stateOrProvinceName - 2.5.4.8

S=Ciudad Autónoma de Buenos Aires

countryName - 2.5.4.6

C=AR

Fecha efectiva

thisUpdate

<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

Proxima Actualización

nextUpdate

<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)

AuthorityKeyIdentifier 2.5.29.35

keyIdentifier = <Identificador de la clave de la AC>

(es una cadena de 20 byte que identifica

Unívocamente la clave pública de la AC ONTI que firmó el certificado.)

Id. de clave=70 ba 03 71 7a d8 10 e4 ee 52 b5 7f 32 8f 9f 6c 2e f7 84 0d

Número de CRL (CRL Number)

OID - 2.5.29.20

Número de la CRL

Indicador Delta CRL

Delta CRL Indicator - 2.5.29.27

Delta CRL

Puntos de Distribución del emisor (IssuingDistributionPoints)

IssuingDistributionPoints - 2.5.29.28

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl

[2]Punto de distribución CRL

Nombre del punto de distribución:

Nombre Completo: Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl

Solo Contiene certificados de usuario = no

Solo Contiene certificados de la entidad emisora = no

Lista de revocación de Certificados Indirecta = no

Certificados Revocados

Fecha de Invalidez

<fecha y hora UTC>

Serial Number

Número de Serie del Certificado Revocado

ReasonCode

Motivo de la Revocación

Algoritmo de Identificación Huella Digital

SHA1

Versión de CA

V0.0

Siguiente Publicación de lista de revocación

<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

8. ADMINISTRACIÒN DE ESPECIFICACIONES

8.1. Procedimientos de cambio de especificaciones

La presente Política será revisada y actualizada periódicamente por el Certificador y sus nuevas versiones se pondrán en vigencia, previa aprobación de la Autoridad de Aplicación.

8.2. Procedimientos de publicación y notificación

Una copia de la versión vigente de la presente Política de Certificación se encuentra disponible en forma pública y accesible a través de Internet en el sitio web http://pki.jgm.gov.ar/cps/cps.pdf

Una vez que la Autoridad de Aplicación notifique al Certificador la aprobación de las modificaciones a la Política de Certificación, éste procederá a su publicación en el sitio web antes mencionado.

8.3. Procedimientos de aprobación

La presente Política de Certificación, así como cualquier modificación a efectuar a la misma o cualquier cambio en los datos relativos a su licencia, serán sometidos a aprobación por parte de la Autoridad de Aplicación.

Historia de las revisiones:

Versión y Modificación Fecha de emisión Descripción Motivo del Cambio

Versión 1.6

22/09/2010

Nota: Cada nueva versión y/o modificación suplanta a las anteriores, resultando sólo vigente la última, la que está representada por

BIBLIOGRAFÍA

[1] Alcazar Díaz de Léon, L., Castillo Camacho, D., & Luna-Reyes, L. F. (2006, May 25-27). *Análisis de la funcionalidad de los portales de gobierno estatal en México*. Paper presented at the XIX Congreso Latinoamericano de Estrategia, Cholula, México.

[2] Ambite, J. L., Arens, Y., Bourne, W., Feiner, S., Gravano, L., Hatzivassiloglou, V., et al. (2002). *Data Integration and Access*. In W. J. McIver & A. K. Elmagarmid (Eds.), Advances in Digital Government. Technology, Human Factors, and Policy. Norwell, MA: Kluwer Academic Publishers.

[3] Andersen, D. F., & Dawes, S. S. (1991). *Government Information Management. A primer and Casebook.* Englewood Cliffs, NJ: Prentice Hall.

[4] Andersen K.V., Henriksen, H.Z. (2006). *E-government maturity models: Extension of the Layne and Lee model*. Government Information Quarterly, vol. 23, pp. 236-248.

[5] Andrade, Andre (2009). *The Strategic Planning and ICT in the Brazilian Justice*, Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance, ACM , pp. 91-96.

[6] ASQ Standards Group: *ISO 9000:2000 Product Support Initiative*. [En línea] 2004. http://qualitypress.asq.org/iso9000/ISO_Curves.pdf.

[7] Bajjaly, S. T. (1999). *Managing Emerging Information Systems in the Public Sector.* Public Performance & Management Review, 23(1), 40 - 47.

[8] Barki, H., Rivard, S., & Talbot, J. (1993). *Toward an assessment of software development risk*. Journal of Management Information Systems, 10, 203-223.

[9] Barrett, K., & Greene, R. (2000). *Powering Up: How Public Managers Can Take Control of Information Technology.* Washington, DC: Congressional Quarterly Press.

[10] Bellamy, C. (2000). *The Politics of Public Information Systems*. In G. D. Garson (Ed.), Handbook of Public Information Systems. New York: Marcel Dekker.

[11] Brown, M. M. (2000). Mitigating the Risk of Information Technology Initiatives: Best Practices and *Points of Failure for the Public Sector*. In G. D. Garson (Ed.), Handbook of Public Information Systems. New York: Marcel Dekker.

[12] Brown, M. M. (2001). *The Benefits and Costs of Information Technology Innovations: An Empirical Assessment of a Local Government Agency*. Pubic Performance & Management Review, 24(4), 351 - 366.

[13] Brown, M. M., & Brudney, J. L. (2003). *Learning Organizations in the Public Sector? A Study of Police Agencies Employing Information and Technology to Advance Knowledge.* Public Administration Review, 63(1), 30-43.

[14] Caffrey, L. (1998). Information Sharing Between & Within Governments. London: Commonwealth Secretariat.

[15] Chevallerau, F.-X. (2005). *eGovernment in the Member States of the European Union*. Brussels: IDABC eGovernment Observatory.

[16] Corbett C.J., Montes M.J., Kirsch D.A., Alvarez-Gil M.J. (2002) *Does ISO 9000 certification pay?* ISO Management Systems. Special Report.

[17] DANE. (2003). *Modelo de Medición de las Tecnologías de la Información y las Comunicaciones: Estadísticas e Indicadores del Sector Estado y Comunidad.* Bogotá: Departamento Administrativo Nacional de Estadística (DANE).

[18] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease to use, *and User Aceptance of Information Technology*. MIS Quarterly, 13(3), 319-340.

[19] Dawes, S. S. (1996). *Interagency information sharing: Expected benefits, manageable risks.* Journal of Policy Analysis and Management, 15(3), 377-394.

[20] Dawes, S. S., & Nelson, M. R. (1995*). Pool the risks, share the benefits: Partnership in IT innovation.* In J. Keyes (Ed.), Technology trendlines. Technology success stories from today's visionaries. New York: Van Nostrand Reinhold.

[21] Dawes, S. S., & Pardo, T. A. (2002). *Building Collaborative Digital Government Systems. Systematic Constraints and Effective Practices*. In W. J. McIver & A. K. Elmagarmid (Eds.), Advances in Digital Government. Technology, Human Factors, and Policy (pp. 259-273). Norwell, MA: Kluwer Academic Publishers.

[22] Dawes, S. S., Pardo, T. A., Simon, S., Cresswell, A. M., LaVigne, M., Andersen, D., et al. (2004). *Making Smart IT Choices: Understanding Value and Risk in Government IT Investments*. Albany, NY: Center for Technology in Government.

[23] Dawes, S. S., & Prefontaine, L. (2003). *Understanding new models of collaboration for delivering government services*. Communications of the ACM, 46(1), 40-42.

[24] Dawes, S. S., Pardo, T. A., & Cresswell, A. M. (2004). *Designing Electronic Government Information Access Programs: A Holistic Approach*. Government Information Quarterly, 21(1), 3-23.

[25] Deming, W. Edwards (1967), *Walter A. Shewhart, 1891-1967,* American Statistician, Vol. 21, No. 2, pp. 39-40.

[26] Denhardt, R. B. (1999). *The future of public administration*, Public Administration and Management, 4(2):279--292.

[27] Edmiston, K. D. (2003). *State and Local E-Government: Prospects and Challenges.* American Review of Public Administration, 33(1), 20-45.

[28] Faniran S., Olaniyan K. (2009). *e-governance diffusion in Nigeria: the case for citizens' demand.* Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance, ACM, pp. 145-149.

[29] Finger M. (2009). *e-gov and public sector reform: what roles for government in e-government?* Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance, ACM, pp. 1-4.

[30] Fountain, J. E. (2001). *Building the Virtual State. Information Technology and Institutional Change.* Washington, D.C.: Brookings Institution Press.

[31] Garson, G. D. (2004). *The Promise of Digital Government.* In A. Pavlichev & G. D. Garson (Eds.), Digital Government: Principles and Best Practices (pp. 2-15). Hershey, PA: Idea Group Publishing.

[32] Gil-García, J. R. (2005). *Exploring the Success Factors of State Website Functionality: An Empirical Investigation*. Paper presented at the National Conference on Digital Government Research, Atlanta, GA.

[33] Gil Garcia Luis, Luna Reyes (2006). Modelo integral de evaluación del gobierno electrónico: una propuesta preliminar. *Proceedings of the 10th Annual International Conference on Digital Government Research: Social Networks: Making Connections between Citizens, Data and Government*. ISBN: 978-1-60558-535-2.

[34] Gil-García, J. R., & Luna-Reyes, L. F. (2003). *Towards a Definition of Electronic Government: A Comparative Review.* In A. Mendez-Vilas, J. A. Mesa Gonzalez, J. Mesa Gonzalez, V. Guerrero Bote & F. Zapico Alonso (Eds.), Techno-legal Aspects of the Information Society and New Economy: An Overview. Badajoz, Spain: Formatex.

[35] Gil-García, J. R., & Luna-Reyes, L. F. (2006). *Integrating Conceptual Approaches to EGovernment*. In M. Khosrow-Pour (Ed.), Encyclopedia of E-Commerce, E-Governmen and Mobile Commerce (pp. 636-643). Hershey, PA: Idea Group Inc.

[36] Gil-García, J. R., & Pardo, T. A. (2005). *E-Government Success Factors: Mapping Practical Tools to* Theoretical Foundations. Government Information Quarterly, 22(2), 187–216.

[37] Gupta, M. P., & Jana, B. (2003). *E-Government Evaluation: A Framework and a Case Study.* Government Information Quarterly, 20(4), 365-387.

[38] Harris, N. D. (2000). *Intergovernmental Cooperation in the Development and Use of Information Systems.* In G. D. Garson (Ed.), Handbook of Public Information Systems. New York: Marcel Dekker.

[39] Heintze, T., & Bretschneider, S. (2000). *Information Technology and Restructuring in Public Organizations: Does Adoption of Information Technology Affect Organizational Structures, Communications, and Decision Making*? Journal of Public Administration Research and Theory, 10(4), 801-830.

[40] Holden, S. H., Norris, D. F., & Fletcher, P. D. (2003). *Electronic Government at the Local Level: Progress to Date and Future Issues.* Public Performance and Management Review, 26(4) 325-344.

[41] Iribarren, M., Concha, G., Valdés, G., Solar, M., Villarroel, M.T., Gutiérrez, P., Vásquez, A. (2008). *Capability Maturity Framework for e-Government: A Multi-dimensional Model and Assessing Tool*. In: Wimmer, M.A., Scholl, H.J., Ferro, E. (Eds.), EGOV 2008. LNCS, vol. 5184, pp. 136-147. Springer Verlag, Berlin et al.

[42] ISO/IEC TR 15504-1:1998 Information Technology – Software Process Assesment – Part 1: Concepts and Introductory Guide. [En línea] http://www.iso.org/iso/iso_catalogue/catalogue_

[43] Jiang, J., & Klein, G. (2000). *Software development risks to project effectiveness*. The Journal of Systems and Software, 52, 3-10.

[44] Kaplan, D., Krishnan, R., Padman, R., & Peters, J. (1998). *Assessing Data Quality in Accounting Information Systems*. Communications of the ACM, 41(2), 72-77.

[45] Kasse, T. *Practical insight into CMMI®*.(2004). Artech House Publishers.

[46] Kraemer, K. L., King, J. L., Dunkle, D. E., & Lane, J. P. (1989). *Managing Information Systems. Change and Control in Organizational Computing.* San Francisco, CA: Jossey-Bass.

[47] Klein, H. K. (2000). *System Development in the Federal Government: How Technology Influences Outcomes*. Policy Studies Journal, 28(2), 313.

[48] Landsbergen, D. J., & Wolken, G. J. (2001). *Realizing the Promise: Government Information Systems and the Fourth* Generation of Information Technology. Public Administration Review, 61(2), 206-220.

[49] La Porte, T. M., Demchak, C. C., & de Jong, M. (2002). *Democracy and Bureaucracy In The Age Of The Web: Empirical Findings and Theoretical Speculations.* Administration and Society, 34(4), 411-446.

[50] Mahler, J., & Regan, P. M. (2003). *Developing Intranets for Agency Managemen*t. Public Performance and Management Review, 26(4), 422-432.

[51] Mutafelija B., Stromberg H. (2003). *Systematic Process Improvement using ISO 9001:2000 and CMMI.* Artech House Computing Library.

[52] Norma ISO 9000. [En línea] http://www.iso.org/iso/iso_catalogue/catalogue_.

[53] Pekkola S., Wideroos K., (2010). *"What We Cannot Speak about We Must Pass over in Silence" - (In)correctly Arguing and Comparing the Costs of IT Investments in Public Sector*. EGOVIS'10, Proceedings of the First international conference on Electronic government and the information systems perspective, pp. 22-31.

[54] Piattini Mario et al (2008). *CompetiSoft. Mejora de Procesos Software para Pequeñas y Medianas Empresas y Proyectos.* Editorial Ra-Ma.

[55] Redman, T. C. (1998). *The Impact of Poor Data Quality on the Typical Enterprise*. Communications of the ACM, 41(2), 79-82.

[56] Rocheleau, B. (2003). *Politics, Accountability, and Governmental Information Systems*. In G. D. Garson (Ed.), Public Information Technology: Policy and Management Issues (pp. 20-52). Hershey, PA: Idea Group Publishing.

[57] Rossel P, Finger M. (2007). *Conceptualizing e-Governance.* Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance, ICEGOV 2007, ACM, pp. 399-407.

[58] Sepúlveda T., M. A., Gutiérrez G., P., & Vásquez V., Á. (2006). *Gobierno Electrónico en Chile 2000-2005: Estado del Arte II.* Santiago: Maval Ltda.

[59] Shewhart, Walter A. (1939) *Statistical method from the viewpoint of quality control*. ISBN 0-486-65232-7.

[60] Souza A., Agante P., Borges Gouveia L., (2010). *Governmeter: monitoring government performance: a web based application proposal*, EGOVIS'10, Proceedings of the First international conference on Electronic government and the information systems perspective, pp. 158-165.

[61] Thomas, J. C., & Streib, G. (2003). *The New Face of Government: Citizen-Initiated Contacts in the Era of E-Government*. Journal of Public Administration Research and Theory, 13(1), 83-101.

[62] Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). *Linking Citizen Satisfaction with EGovernment and Trust in Government.* Journal of Public Administration Research & Theory, 15(3), 371-391.

[63] West, D. M. (2004a). *E-Government and the Transformation of Service Delivery and Citizen Attitudes.* Public Administration Review, 64(1), 15-27.

[64] Wilson J.P. *An Examination of the Economic Benefits of Iso 9000 and the Baldridge Award to Manufacturing Firms*. University of Pittsburgh - PhD Thesis, 2004.